Lions and Tigers and Bears, oh my! Global Legal Risks in Cybersecurity Investigations[1]

Brian Hengesbaugh, Global Chair of Privacy and Security, Baker McKenzie

In the classic movie "The Wizard of Oz," Dorothy, Scarecrow and Tinman walk through the forest while expressing great concern about the "lions and tigers and bears, oh my!" they may face on their journey to Oz. Companies experiencing global ransomware and cyberattacks can experience similar emotions as they grapple with increasingly complex global legal risks. Across the globe, local legislatures and regulatory authorities have established a multitude of different and sometimes conflicting legal obligations that can impact not only the timing and content of mandatory notifications about the incident but also the shape of the cybersecurity investigation itself. The challenge is particularly acute with cyber incidents, given time pressures, customer demands, adverse media attention and business disruption.

To help companies prepare, it can be helpful to organize the global legal risks arising in cyber incident investigations into categories outlined below. The requirements for individual companies may vary depending on their geographic footprint, industry vertical, operations and other factors.

Lions: Mandatory incident notification obligations

Mandatory notification obligations are often among the first legal issues a company needs to face in a global cyber incident. Typically, a company may know little about the scope of the incident in the first few days after discovery. Still, the clock can start ticking early, and the company knows it could be judged for failing to act with sufficient speed and transparency in making any required notifications. At the same time, it faces a real risk that it could make overly broad notifications to customers or others beyond what is needed, which is typically not helpful for the customers, other notice recipients, or the company's risk profile. Alternatively, given that little is known with certainty, the company faces the corresponding early notification risk of inadvertently notifying improperly (either by notifying fewer or different notice recipients than needed or identifying fewer or different data categories that are impacted). Such improper notification can give rise to potential claims of fraud and misrepresentation. The company also must address these issues in a compressed timeframe within a complex global legal environment that now carries various notification regulatory requirements with different purposes, scope, and timing requirements including the following:

Data protection and privacy breach notice requirements

Data protection and privacy breach notification obligations are proliferating globally. These laws generally require notification to data protection authorities, individuals, and others if the company becomes aware of a data breach impacting personal data about customers, employees or other individuals. For example, more than 35 jurisdictions now have requirements to make such data protection authority notifications within 72 hours, while many other laws establish "as soon as reasonably possible" and other similar timing standards.

SEC/Public company notice obligations

Public company and securities regulations increasingly require public companies to notify securities regulators and investors if a cyber incident is material to an investor's decision. These duties can attach regardless of whether any "personal data" is impacted by the incident and given that a company may be aware of materiality before it becomes aware of specific personal data impact, the company needs to consider these standards and timelines independently from data privacy breach notifications. For example, the U.S. Securities and Exchange

[1] Published in IAPP Privacy Advisor, January 2024

Commission has adopted a final rule that requires notification within four days of a determination that a cyber incident is material, and other jurisdictions are adopting similar requirements.

Financial, health care, telecommunications and other regulatory notice obligations

Various regulatory authorities in the financial services, health care, telecommunications and other regulated verticals are increasingly establishing notification duties for regulated entities. For example, the Reserve Bank of India has a one-hour rule for reporting cyber incidents in the banking sector. The China Interim Measures for Reporting of Information Security Incidents of Healthcare Quality require licensed health care institutions to report extremely serious information security incidents concerning the quality of medical treatment to public health authorities within two hours after discovery. And the French Telecommunications Code requires certain electronic communications service providers to notify the National Authority for Information Systems' Security of certain cyber incidents without delay.

Cybersecurity and critical infrastructure reporting obligations

Cybersecurity and critical infrastructure agencies increasingly require notifications for entities within the scope of their authority. For example, the Australian Cyber Security Centre requires data centers and other critical infrastructure assets to report within 12 hours of becoming aware of an incident. The Indian Computer Emergency Response Team requires a broadly defined group of companies, including service providers and intermediaries, to make a notification of certain cyber incidents within 6 hours. The European Union NIS 2 Directive, which EU member states will implement by October 2024, requires certain essential and important entities to report significant incidents to the local Computer Security Incident Response Team or other competent authority within 24 hours. In addition, pursuant to the U.S. Cyber Incident Reporting for Critical Infrastructure Act of 2022, the Cybersecurity and Infrastructure Security Agency is engaged in mandatory rulemaking that is expected to require covered entities to report covered cyber incidents to CISA within 72 hours and ransomware payments within 24 hours.

Contractual obligations

Apart from regulations, companies often have numerous contractual duties to report cyber incidents to customers, financial institutions, or others. For example, the Payment Card Industry rules, applicable to merchants through contractual agreements, generally require immediate notification of cyber incidents impacting cardholder information to payment card brands and acquirers (merchant banks). Companies may also have short timelines for notification within customer agreements, particularly if they act as data processors/service providers/agents to corporate customers for personal data.

To the extent feasible, companies should plan ahead to identify the different categories of data protection notification obligations that may attach in the event of a cyber incident. At the time of an incident, companies should engage in close coordination of a global notification strategy to ensure that notifications are consistent from a content and timing perspective and take into account potential privilege issues with disclosures to third parties.

Tigers: Legal restrictions on data collection, use and transfer

The investigation of a global cyber incident often involves the collection, use and transfer of data, such as data contained in images of servers and other devices, data collected from email systems and applications, and a wide variety of data collection in the form of indicators of compromise and other evidence, including IP addresses, domain names, file hash values or other information about patterns of behavior. The data may be collected from systems or networks outside the home country where the parent company is located, and the company may need

to engage third-party forensics, e-discovery, or other providers to assist with data collection, use, analysis and transfer. Depending on the specifics of the situation, including geographic footprint, categories of data and other factors, the company may need to address various local legal restrictions on these activities, such as:

Data protection and privacy

The company should confirm that employees, customers or other data subjects about whom personal data is collected, used and transferred in the context of a cyber incident have been provided with appropriate privacy notices and that the company has a sufficient legal basis for processing, including special considerations to the extent health/medical or other sensitive personal data is at issue. The company should also consider proportionality and data minimization requirements and consider documenting a data protection impact assessment depending on the situation. In addition, the company may need to address cross-border data transfer restrictions, including implementing appropriate data protection contractual obligations with third-party service providers, such as forensics or e-discovery.

Wiretapping and electronic communications

To the extent the investigation involves the collection and review of email or other communications, the company should confirm that it addresses any applicable local wiretapping and electronic communications requirements that prohibit or restrict the interception, review or recording of communications, in addition to ensuring that data subjects have been appropriately notified about and/or provided consent to such potential monitoring. For example, unless the company effectively prohibits employee personal use of company email systems, the German Telecommunications Act generally establishes two-party consent requirements for reviewing email communications. Similarly, the Brazilian Federal Constitution, the Communications Interception Act and other provisions establish the right to privacy and inviolability of electronic and other communications that require consent or other legal basis for collection.

Labor and employment law

Where the company has works councils or other employee-representative bodies, it may have obligations under labor law and labor agreements to engage in notification or prior consultations with such employee representative bodies. For example, the German Works Constitution Act is a federal law in Germany that governs the right of employees to form a works council, pursuant to which many companies have reached agreements on the specifics of notification, consultation, and co-determination procedures for employee monitoring and other activities related to cyber investigations.

In the midst of an actual cyber incident, companies may have limited ability to conduct meaningful compliance efforts for these types of data restrictions and instead must engage in risk-based decision-making to manage the most significant risks in a practical manner while facilitating an effective cybersecurity investigation.

Bears: Potential conflicts of law for disclosures to home law enforcement or other authorities

In specific circumstances, the company's investigation may potentially conflict with local anti-investigatory or "blocking" statutes or other local considerations that create criminal or other substantial local law risk. Key examples of these types of conflicts of law are as follows:

Anti-investigatory or 'blocking' statutes

These statutes have been adopted with the specific intention to interfere with foreign (i.e., nonlocal) government investigations. For example, French Law No. 80-538 of 16 July 1980 generally prohibits the communication/transfer of documents or information that can lead to the establishment of evidence in a foreign judicial or other proceeding. Similarly, Article 271 of the Swiss Criminal Code generally prohibits the collection of evidence located in Switzerland intended for use in proceedings outside of Switzerland. These requirements could become relevant to the extent that the company collects data in any of these local territories and exchanges such information with the FBI or other law enforcement or regulatory authorities in its home jurisdiction.

Bank secrecy and professional confidentiality

Local bank secrecy or other industry-specific confidentiality duties may apply to banking, health care, and other regulated data. For example, the Greece Banking Legislative Decree 1059/1971 generally prohibits local bank operations from sharing customer deposit account information with third parties and affiliated companies, including parent companies, and such restrictions cannot be waived by customer consent. Similarly, Section 47 of the Singapore Banking Act generally prohibits local bank operations from disclosing or transferring customer information to locations outside of Singapore.

'State secrets' and other restrictions

Other requirements may apply, depending on the jurisdiction at issue. For example, China has adopted the Law on Guarding State Secrets that may apply to the extent any data or documents relate to sensitive sectors or senior government officials. Regardless of any purported individual consent, the transfer of such data outside can give rise to potential criminal liability.

To the extent that any particular investigation gives rise to these types of potential conflicts of law described above, they may present some acute challenges. Although, in most instances, a company may assess an overriding need to proceed with its investigation, the company may make certain strategic decisions, such as whether or how to perform certain portions of the investigation in the local jurisdiction where the data resides or how to engage with law enforcement in its home country in a manner that could help to reduce these local legal risks.

Recommendations

Given the complexities of the multijurisdictional legal environment, companies should conduct an assessment as part of their pre-incident planning process to identify potentially applicable requirements across all three categories of obligations as described. To the extent feasible, companies should also align their overall data compliance frameworks to help mitigate the risks associated with these varying requirements and incorporate some of the complexities posed by the legal requirements into their incident response plans and tabletop exercises. While no amount of planning can solve all of the problems, thoughtful planning can reduce some of the understandable concerns and otherwise mitigate the concerns of facing the lions, tigers and bears arising from global legal risks in a cybersecurity attack.