Baker McKenzie.

Lions and tigers and bears, oh my! Global legal risks in cybersecurity investigations

Privacy + Security Forum, Washington, DC | May 10, 2024

Brian Hengesbaugh, Partner, Baker McKenzie
Scott Jones, Senior Counsel, Johnson & Johnson
Mary Ann Le Fort, Chief Privacy Officer, Priceline.com

Agenda

00 Welcome

01 Lions: Mandatory incident notification obligations

02 Tigers: Legal restrictions on data collection, use and transfer

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

04 Oh my: Practical tips to avoid issues in cross border cybersecurity investigations

Speakers

Brian Hengesbaugh
Partner
Baker McKenzie

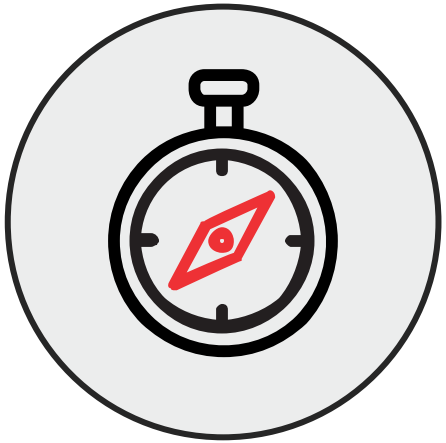
Mary Ann Le Fort
Chief Privacy Officer
Priceline.com

Scott Jones
Senior Counsel, Cybersecurity
Johnson & Johnson

“Different and sometimes conflicting legal obligations can impact not only the timing and content of mandatory notifications about the incident but also the shape of the cybersecurity investigation itself.”

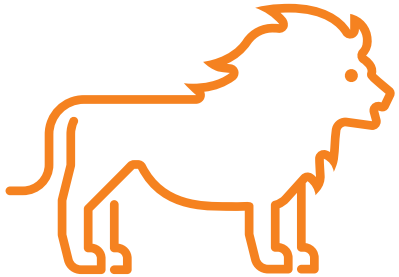
“Toto, I've a feeling we're not in Kansas anymore… We must be over the rainbow!”

01 Lions: Mandatory incident notification obligations



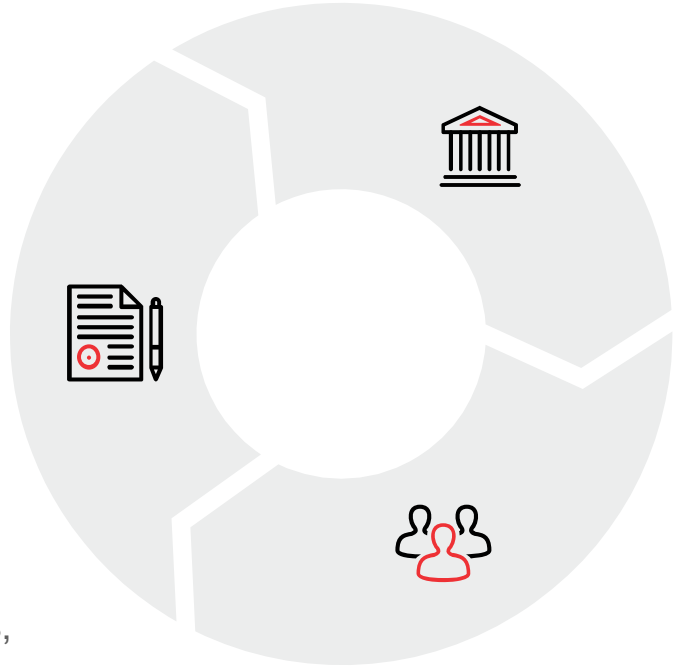
Incident notification obligations

- among the first legal issues a company needs to face in a global cyber incident
- notification triggers and deadlines may vary creating complexities in formulating a notification strategy



contractual notification obligations

apart from regulations, companies often have contractual duties to report cyber incidents to customers, financial institutions, or others, including payment card industry (PCI) requirements



privacy notifications to authorities

some of the fastest notification duties are to data protection and other authorities (e.g., 72 hours in EU, 6 hours in India, 1 hour under draft rules in China)

privacy notifications to individuals

all 50 states and most major economies require notification to affected individuals for certain types of cybersecurity incidents

Notification requirements: endless variations

	Applicability	Trigger	Timing
SEC Cyber Rules	*Public companies*	*"Material" incident*	*Within 4 days of materiality determination*
HIPAA Breach Notification Rule	*"Covered Entities" and "Business Associates"*	*If breach affect 500+ individuals*	*Without unreasonable delay and in no case later than 60 days following discovery of breach*
Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)**	*"Covered Entities" in a critical infrastructure sector*	*"Substantial cyber incident"*	*Within 72 hours of when a covered entity reasonably believes an incident occurred*
EU General Data Protection Regulation (GDPR)	*Controllers that process EU citizens' personal data*	*"Personal data breach", unless unlikely to result in a risk to personal rights/freedoms*	*Within 72 hours of becoming aware of breach*
India's CERT Directions	*Service providers, intermediaries, data center, and others*	*Any real or suspected adverse cybersecurity incident that violates applicable security policy*	*Within 6 hours of detection or being notified of incident*

**CIRCIA rulemaking process commenced in March 2024; expected to come into effect by October 2025

“You are under the unfortunate delusion that simply because you run away from danger, you have no courage. You're confusing courage with wisdom.”

Notifications: Striking the right balance

- Failure to disclose or inadequate disclosure can have legal or regulatory consequences
- Authorities may help to contain breach or understand threat actor
- Attempting to conceal notifiable breach can give rise to significant consequences
- Timely notification can help affected individuals and entities take steps to mitigate

- May know little about the scope of the incident at time when notifications are required
- Overly broad notifications may be unhelpful or confusing to customers or employees
- Unnecessary or improper disclosures may increase company's legal risk or give rise to potential claims of fraud and misrepresentation
- Disclosure to single regulator may set off a chain reaction

Case Study #1

A publicly-traded US-headquartered B2B global company experiences a ransomware incident. The company provides data management services (including data storage) to multinational company customers globally. The ransomware is widespread and affecting the company's data centers in China, India, Germany, and the US. The company's customers cannot access their data.

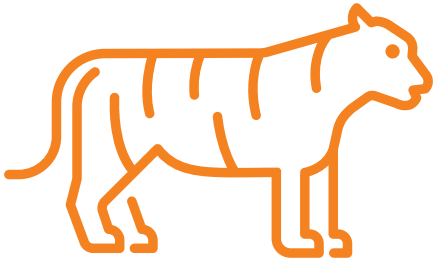
1. Is this incident "material" under the SEC Cyber Rules?
2. Should this incident be reported to India's CERT-In authorities within **6 hours**?
3. Have we triggered GDPR reporting obligations?

02 Tigers: Legal restrictions on data collection, use and transfer

Data protection restrictions

Wiretapping and electronic communications

Labor and employment law



Legal restriction impact on data collection

Data Sources
Email systems
Enterprise applications
Mobile and other devices
Servers
Networks devices

Categories of data subjects and protected persons
Employees/ Contractors
Consumers/ Customer Contacts
Vendor/ Business Partner Contacts
Patients/ End Users
Local companies
Public generally

Data protection and privacy restrictions

Notice

Have individuals about whom personal data is collected, used and transferred in the cyber investigation been provided with appropriate privacy notices?

Data protection impact assessment

Consider documenting collection, use and trasnfer of personal data in an impact assessment.

Proportionality

Consider whether data minimization or purpose limitation strategies mitigate concerns.

Cross border transfers

Address cross-border data transfer restrictions, including implementing contractual obligations with third-party service providers, e.g., forensics or e-discovery

China: Crossborder Data Transfers

Three Options:

Security Assessment

Required for:
- Critical information
- Large amounts of data or transfers
- Important data

Conducted by CAC
Requires risk assessment
Specific data transfer agreement with overseas recipient

Standard Contractual Clauses

Available when Security Assessment is not required

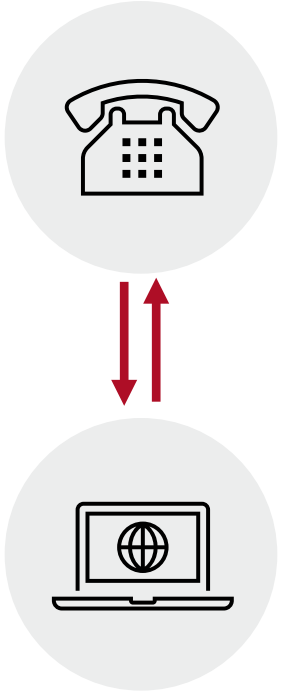
Requires personal information protection impact assessment
Export contract to be strictly based on standard contract

Certification

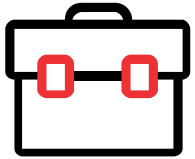
Little current guidance from CAC

Wiretapping and electronic communications restrictions

- ❑ Address any applicable local wiretapping and electronic communications requirements that prohibit or restrict the interception, review or recording of communications
- ❑ Ensure that data subjects have been notified about and/or provided consent to potential monitoring
- ❑ Identify whether one- or two-party consent for monitoring is required



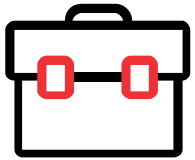
Labor and employment law considerations



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, many companies have reached agreements pursuant to the German Works Constitution Act on the **specifics of notification, consultation, and co-determination procedures** for employee monitoring and other activities related to cyber investigations

Case Study #2

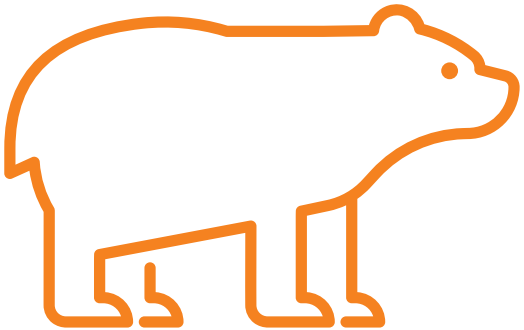


A multinational company's Data Loss Prevention (DLP) system alerts the InfoSec team that large amounts of patient data are being exfiltrated from the company's systems. The alerts are tied to one Chinese employee and one German employee, both of whom deny any wrongdoing and claim that their accounts must have been taken over by an unauthorized actor. The company initiates a forensics investigation, which involves collecting both employees' company-issued devices, as well as reviewing their network activity and emails. Company headquarters engages US-based external counsel and forensics provider to direct and carry out this investigation, respectively.

1. Can the company collect the employees' devices and emails lawfully?
2. Does the company need any type of consent from the employees to initiate this investigation?
3. Can the company transfer the devices (or forensic images of the devices) and emails to the US? Is there any criminal liability associated with this transfer?

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

Potential conflict of law restrictions



A company's investigative activities may potentially conflict with:

- Local anti-investigatory or "blocking" statutes
- Bank secrecy or other professional confidentiality rules
- State secrets restrictions

Bank secrecy or other professional confidentiality rules

Local bank secrecy or other industry-specific confidentiality duties may restrict the use of regulated data

Greece Banking Legislative Decree 1059/1971 prohibits local banks from sharing customer deposit account info with third parties and affiliates and can’t be waived by customer consent

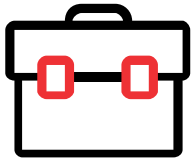
Similar restrictions may exist for health data or in other regulated industries

“State Secrets” and other restrictions

Other laws may restrict the flow of information considered to be sensitive by the state:

- China has adopted the Law on Guarding State Secrets applying to any data or documents related to sensitive sectors or senior government officials. Regardless of any purported individual consent, the transfer of such data outside the jurisdiction can give rise to potential criminal liability

Case Study #3



A financial institution with headquarters both in the US and in Switzerland is conducting an internal investigation into several employees belonging to one of their French branches. Allegedly, these employees all used their personal devices to log into the financial institution's internal systems and look up information about the branch's most affluent clients in order to subsequently extort these clients. Both US and Swiss financial regulators have initiated investigations and issued subpoenas for information, including the contents of the French employees' searches and related communications.

1. Assuming that the company's log files and emails are stored in Switzerland, can the company provide the requested information to Swiss regulators? What about US regulators?
2. Does the answer to the question above change if we assume the company's log files and emails are stored in the US?
3. What are the risks if the company refuses to provide the information to US regulators?

04 Oh my: Practical tips to avoid issues in cross border cybersecurity investigations

Follow the Yellow Brick Road

- Conduct legal analysis as part of the pre-incident planning process to identify potentially applicable requirements
- Align overall data compliance elements (e.g., privacy notices/consents) to help mitigate associated risks
- Incorporate some of the complexities posed by the legal requirements into incident response plans and tabletop exercises

Questions

Baker McKenzie Resources

Connect on Tech Blog and Podcast Series

Our blog and podcast series covering a broad range of topics such as data privacy and security, cybersecurity, digital innovation and transformation, generative AI and machine learning and other topics. The podcast features short 10-minute interviews with Baker McKenzie attorneys across the globe to discuss practical tips and the impact of data and technology on business.

- SEC Adopts Final Cybersecurity Rules
- Hacker attempts to use SEC rules to further exploit victims
- New York State Sets the Bar for Cybersecurity Requirements
- CISOs, Internal Accounting Controls, Crown Jewels and Disclosure Procedures: Peeling Back The Onion of the Solar Winds Enforcement Action
- Podcast Episode: The SEC's Final Cybersecurity Rules - A Look at Evolving Risks in the New Age
- US Government to Restrict Sharing of US Bulk Sensitive Personal Data With Certain "Countries of Concern"

Global Data Privacy & Cybersecurity Handbook (Updated Jan. 2024)

It has never been easier for companies to collect, copy and transfer personal data around the world. But at the same time, the introduction of a wide range of privacy and security laws worldwide imposes complex and often inconsistent privacy and data protection standards impacting on multinational companies. Our Global Privacy & Cybersecurity Handbook provides detailed overviews of the increasingly complex and sophisticated privacy and data protection standards in over 50 countries.

External Resources

- FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements
- Data Privacy And Cybersecurity Issues In Mergers And Acquisitions (Forbes article)
- DHS-CISA Updates: https://www.cisa.gov/
- IBM Cost of a Data Security Breach Report 2023.
- Crowdstrike 2023 Threat Hunting Report
- 2023 IC3 Annual Internet Crime Report (Released March 2024)
- Verizon 2023 Data Breach Investigation Report
- SentinelOne Watchtower End of Year 2023
- ChatGPT Security Risks: A Guide for Cyber Security Professionals (Cybertalk.org)
- World Economic Forum Global Risks Report 2024
- ISACA State of Cybersecurity 2023

Baker McKenzie.

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com