Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell, Leah Schloss, Maury Riggan and Jason C Chipman

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-223-7

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

RICHARD DENATALE

HUNTON ANDREWS KURTH LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its third edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Part I

A 'Typical' Cyber Investigation

4

Complying with Breach Notification Obligations in a Global Setting: A Legal Perspective

Aaron P Simpson and Adam H Solomon[1]

Technological advances have led to previously unimaginable computing capabilities. As these advances have continued to evolve in recent years, so too have privacy and data security concerns relating to the appropriate use and protection of personal information by global organisations. These concerns have become fundamental questions in the current Information Age as security breaches are reported in major publications across the globe almost every day. In many cases these media stories result from legal obligations imposed on organisations to notify the public or regulators, or both, in the event of a data breach. In this chapter, we provide an overview of these notification obligations, and recommendations regarding optimal approaches to managing the fast-changing global legal environment.

Breach laws around the globe

United States

The United States maintains the most mature and actively enforced framework of data breach requirements in the world. Although there is no national breach notification law, all 50 states, plus the District of Columbia, Guam, Puerto Rico and the US Virgin Islands, have enacted data breach notification laws. These state laws generally are designed to require organisations to notify affected residents of compromises to the security, confidentiality or integrity of 'personal information' maintained by those organisation. Unlike in many other jurisdictions, US laws typically include a circumscribed definition of 'personal information' focused as data elements perceived to be sensitive. The majority of states also require notification to regulators if the breach affects a specified number of residents.

1 Aaron P Simpson is a partner and Adam H Solomon is an associate at Hunton Andrews Kurth LLP.

In addition to the state breach laws, there are also sector-specific breach notification requirements at the federal level. For example, banks and other financial institutions[2] and certain healthcare organisations and their service providers[3] are subject to comprehensive breach notification requirements. Although a number of state breach notification laws exempt organisations subject to the federal rules from coverage, many state breach laws contain no such pre-emption and require businesses to comply with both the state and federal breach requirements. Further, for publicly traded companies, some security incidents can rise to the level of reportable events. In these cases, it may be necessary to disclose the breach to investors and the US Securities and Exchange Commission.[4]

Canada

Breach notification in Canada was governed historically at the provincial level, with only Alberta's provincial data protection law imposing mandatory breach notification obligations across industry sectors, and certain other provinces requiring notification for breaches involving health data. However, this changed when Canada's federal Personal Information Protection and Electronic Documents Act was amended to require organisations to provide breach notification to affected individuals and the federal Privacy Commissioner as of 1 November 2018. The relevant implementing regulations specify the content, form and manner of breach notification, and require notification as soon as is feasible after determination that a breach has occurred.

European Union

The General Data Protection Regulation (GDPR) imposes a data breach notification requirement throughout the European Union.[5] The GDPR sets a low bar for notification, requiring a controller to notify the competent supervisory authority of a personal data breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.[6] Several EU supervisory authorities have developed their own breach reporting forms that organisations

2 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736 (29 Mar 2005) (codified at 12 CFR pt 30).

3 Health Breach Notification Rule; Final Rule, 74 Fed. Reg. 42,960 (25 Aug 2009) (codified as amended at 16 CFR pt 318 (2015)).

4 In the United States, public companies have an obligation to disclose material information to investors, particularly when that information concerns cybersecurity risks or incidents. Public companies may be required to make such a disclosure in periodic reports in the context of risk factors, management's discussion and analysis of financial results, description of the company's business, its material legal proceedings, its financial statements, and with respect to board risk oversight. Sec. & Exch. Comm'n, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Interpretation, 83 Fed. Reg. 8166 (26 Feb 2018).

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR). Prior to implementation of the GDPR, there was no uniform data breach notification obligation across the Member States, but certain Member States had enacted their own data breach notification rules and others' relevant data protection authorities had issued breach notification guidance to organisations.

6 GDPR, Article 33.

must submit online to report personal data breaches.[7] A controller also is required to notify affected individuals of a personal data breach, but only if the breach is likely to result in a high risk to the rights and freedom of natural persons.[8] Contrast this approach with that taken in the United States. The European Union uses the full extent of the meaning of 'personal data' under the GDPR in the breach context, and notification hinges on the risk associated with a breach event. In addition, the default notice obligation, when applicable, is to the regulator, not the individual. Notice to individuals is only required when a higher threshold level of harm is likely to result from the breach.

In addition to the GDPR requirements, many individual EU Member States maintain sector-specific laws that impose breach reporting requirements on covered organisations, such as telecommunications providers. The European Union also recently enacted a framework for reporting cybersecurity incidents involving certain critical infrastructure businesses. Directive (EU) 2016/1148 on the Security of Network and Information Systems (the NIS Directive) requires operators of essential services and digital service providers to report to regulators certain cybersecurity incidents that have a substantial effect on their services.

Asia-Pacific

In recent years, there has been a proliferation of data breach notification laws in the Asia-Pacific region. Australia, China, the Philippines and South Korea are examples of jurisdictions that now require breach notification. Some jurisdictions (e.g., India and South Korea) maintain sector-specific breach notification rules, such as for financial institutions or information technology companies. Moreover, the harm thresholds for notification and timing requirements specified by the laws vary widely by country and industry sector.

Latin America

Although several countries in Latin America have enacted comprehensive data protection laws, relatively few have mandatory breach notification requirements. Those that have include Mexico,[9] Colombia [10] and Costa Rica.[11] In Argentina, breach notification to affected individuals or regulatory authorities is not mandatory, but organisations are required to maintain a ledger of data breaches, which must be provided to the data protection authority (DPA)

7 For example, Ireland's Office of the Data Protection Commissioner has developed an online form and portal for organisations to report personal data breaches to the Commissioner, available at https://forms.dataprotection.ie/report-a-breach-of-personal-data.

8 GDPR, Article 34.

9 Mexico requires notification to affected individuals without delay in the event of loss, theft or unauthorised disclosure, access, use, processing, modification, damage or destruction to personal information that materially affects the property or moral rights of the affected data subject. Mexico's law does not require regulator notification.

10 Colombian law requires notification to the data protection authority regarding security breaches that pose a risk in the processing of personal information, but it does not require individual notification.

11 In Costa Rica, individual notification is required within five business days of the entity becoming aware of a breach (defined as an 'irregularity' in the processing or storage of personal data, such as loss, destruction, theft or misuse of personal data). The entity is required to notify the data protection authority of the breach (though there is no explicit deadline for regulator notification).

upon request. Effective from August 2020, Brazil's newly enacted data protection law will require notification of breaches to the DPA and, in some cases, affected individuals.

Africa and the Middle East

Relatively few jurisdictions in Africa and the Middle East have mandatory breach notification requirements at this time. Ghana, Lesotho, Mauritius and South Africa are examples of African jurisdictions where breach notification is required. Israel, Qatar and the Dubai International Financial Centre impose mandatory breach notification obligations in the Middle East. Similar to other regions, the laws in Africa and the Middle East vary widely. For example, in Israel, database owners designated as providing an intermediate or high tier of security must notify the relevant regulator (who may require notification to affected individuals), while in South Africa, the relevant regulator and affected individuals must be notified if there are reasonable grounds to believe there has been unauthorised access to or acquisition of personal information.

Key factors in assessing breach notification obligations

When responding to a data security incident, organisations must determine whether the event triggers a notification requirement under applicable laws. The challenge associated with this determination is that there are important distinctions between data breach laws that often come into play when developing a notification strategy. Since the definitions and threshold requirements differ among the laws, creating a 'one-size-fits-all' notification strategy can be difficult. However, there are several important factors to take into account in making this determination from a legal perspective.

Does the incident meet the definition of data breach in relevant jurisdictions?

The definition of a data breach establishes the scope of compromises that are potentially notifiable under the relevant law. In the United States, most state breach laws consider a data breach to occur when the security, confidentiality or integrity of legally cognisable personal information has been compromised as a result of an unauthorised person accessing or acquiring the information. Other breach rules outside the United States have expanded on this definition to recognise additional types of compromises of personal information. For example, the GDPR's definition of a personal data breach covers accidental or unlawful destruction, loss, alteration, unauthorised disclosure of , or access to, personal data.

In practice, understanding whether a given security incident amounts to a data breach under the law can be challenging when the definition of a data breach is complicated by legal jargon, such as when the definition forces companies to interpret when 'unlawful access' or 'a breach of security' has occurred. These undefined and ambiguous terms often lead to confusion and uncertainty, leaving organisations little choice but to focus instead on the general nature of an incident and its potential ramifications in determining whether a notifiable data breach has occurred.

It also is important to be aware of any exceptions contained within the relevant law. For example, nearly all US state breach laws exclude from the definition of a data breach circumstances in which an employee or agent accidentally accesses personal information in the workplace when acting in good faith and on behalf of his or her employer.

Has personal information been affected within the meaning of the law?

Another key factor to consider when evaluating a security incident is whether the compromised information meets the definition of 'personal information' (or its equivalent) within the relevant law. Many breach rules outside the United States have adopted expansive definitions of personal information consistent with data protection laws. However, US data breach requirements often view personal information more narrowly to include an individual's name in combination with specific data elements that are likely to be used by criminals to commit identity theft or financial fraud. Yet even in the United States, states have begun to move towards expanding the personal information covered under their notification requirements to reach new types of data about which individuals are concerned, such as online account access credentials, biometric data, health information and tax return information.

In addition to the elements of personal information affected, organisations also need to consider the format of the compromised data. Some breach laws apply only to data in electronic form, while others are agnostic to format and apply to any personal information, including in hard-copy records.

Is the breach likely to cause harm to individuals?

Most breach laws are designed to require notification only when a data breach is likely to cause a certain threshold of harm to individuals. Under these laws, the notification trigger is based on the potential for harm or risk to individuals. For this reason, organisations responding to a data breach need to consider the potentially harmful consequences of the breach on affected individuals and assess the likelihood of these consequences occurring. Most of the breach rules in the United States, for example, embrace this harm threshold and require notification only when a breach is reasonably likely to result in harm to individuals. Some breach rules are concerned only with the harm associated with identity theft, account fraud or other financial risks, while others view harm more broadly to reach other threats about which individuals may be concerned. For instance, the GDPR's breach notification requirements recognise various types of harm, including physical, material or non-material damage to individuals. Other examples of harm are loss of control over personal data, loss of legal rights, discrimination, reputational damage, loss of confidentiality or any other significant economic or social disadvantage. In assessing the harm associated with a breach, organisations should keep in mind that they may have an obligation under certain breach notification rules to retain records of their harm determination or report the determination to regulators.

Was the affected data encrypted or redacted?

Some breach laws offer notification safe harbours for data breaches involving encrypted or redacted personal information. These safe harbours excuse notification if the affected personal information was encrypted or redacted when compromised. The scope of these safe harbours tends to vary significantly from law to law. For example, several US state breach laws specify the number of digits that must be redacted to meet the safe harbour from notification, while others are silent on the amount of information that may remain intact. Likewise, most US breach laws provide exceptions for encryption to the extent that the relevant decryption key has not been compromised by the breach. Even if a breach law does not include a safe harbour for encryption or redaction, data protection safeguards (e.g., encryption or

pseudonymisation) may reduce the risk of harm to individuals resulting from the breach to render the information useless and excuse notification under an applicable harm threshold.

Notice mechanics

After determining that a notifiable data breach has occurred, the next step is to consider to whom, how and when the notification must be made. Breach laws generally require notification to a combination of the following: (1) affected individuals; (2) regulatory authorities; and (3) other relevant parties, such as consumer reporting agencies or the media, in some cases. While the majority of laws require notification to affected individuals, certain global laws require notification only to regulators, or to affected individuals only after a regulator mandates it.

Timing of notice

An increasingly significant challenge for organisations is the pressure to provide timely notification of data breaches. Nearly all breach notification laws dictate the time frame within which notification must occur. For example, some breach laws require notice to affected individuals or regulators within a specified number of days (e.g., 30, 45 or 60 days), while others provide only a general timing standard (e.g., immediately, in the most expedient time possible or without undue delay). There even may be different requirements within the same law. For example, the GDPR requires notice to regulators no later than 72 hours after becoming aware of a personal data breach and mandates sending individual notification without undue delay. Further, many breach laws allow delaying notification for specific purposes, including if law enforcement authorities request a delay or to determine the scope of the incident. Given the variance of timing requirements across and within the laws, it is imperative to check relevant data breach rules to ensure compliance with applicable timing specifications.

Form and content of notice

Breach laws also often establish requirements regarding the form and content of notice provided to individuals and regulators. For instance, in the United States, most state breach laws specify the following means for providing notice to individuals: (1) written notice, (2) electronic notice under limited circumstances, or (3) substitute notice (consisting of email notice, conspicuous posting on the entity's website and notification to major statement media) if notifying consumers will cost more than a certain amount of money (e.g., US$250,000) or if more than a certain number of individuals (e.g., 500,000) are affected. The GDPR includes a similar concept, whereby a public communication is permissible if notice to individuals would require a disproportionate degree of effort. For notification to regulators, notice usually will be provided through written means, or through the submission of breach notification forms provided by the regulator.

Breach laws also often include specific content requirements regarding the details that must be provided in the notice to regulators and affected individuals. For example, it may be necessary to include in the notice a description of what happened, the nature of an individual's personal information involved, the steps taken to protect the affected personal information from further compromise, and how the entity will assist affected individuals (e.g., providing credit monitoring or fraud prevention services). Certain state breach laws are even more

prescriptive about what needs to be included in the notice and demand disclosures relating to specific recommendations for affected individuals (such as how to obtain free credit reports or sign up for fraud alerts or security freezes) and the contact information for consumer reporting agencies and regulators. Other laws, such as California's breach notification law, go so far as to provide mandatory forms on which notification must be provided to individuals or regulators.[12] In connection with these notification requirements, some organisations establish call centres to help handle enquiries from affected individuals and offer fraud prevention or credit monitoring services, where relevant and available. Some states (e.g., California and Maryland) require their attorney general to provide a copy of this notice to residents and to publish the notice on the attorney general's website.

In providing notification, organisations often need to coordinate with service providers and take a number of logistical steps. It may be necessary, for example, to access the most recent contact information for the affected individuals held on file at the organisation, stand up or procure a call centre, arrange for credit monitoring and identity protection services, engage a service provider to mail or email notifications, develop a website to post a substitute notice, draft supplemental materials such as FAQs and reference guides for individuals, and develop training materials and talking points about the incident. Well-equipped organisations often plan ahead for these notification activities, including by seeking to have these relationships in place and developing template materials before an incident occurs.

Variations in notice obligations for third-party providers

In general, entities that own, license or control information that has been breached typically bear the legal responsibility for notifying affected individuals and regulatory authorities under breach notification laws. In many US states, for example, the data owner is the party who is legally responsible for notifying affected individuals and regulators. Similarly, in the European Union, the controller is the party responsible under the GDPR for notifying individuals and regulators.

In contrast, service providers and other businesses that maintain data on behalf of their customers, or others generally, are responsible under data breach rules for notifying their corporate customers of a reportable breach.[13] Additionally, service providers and data maintenance businesses are required under certain laws to 'cooperate' with their corporate customers during the notification process by, for example, providing information about the breach to the customer. This information can include, for example, the date or approximate date of the breach, the nature of the breach and any steps the service provider has taken or plans to take relating to the breach. This is true in both the United States and the European Union, where processors are required to notify controllers, who in turn are responsible for notifying regulators and data subjects. From a policy perspective, the rationale behind this framework is sound: for notice to be meaningful, it should be provided by the organisation with whom the individual data subject maintains a relationship.

12 See Cal. Civ. Code, Section 1798.82(D).

13 In the European Union, data processors (i.e., those who process personal data on behalf of a data controller) are responsible for providing notice to the data controller of a reportable breach.

Contractual considerations

As discussed above, service providers or processors typically must notify only the data owner or controller in the event of a data breach, and the owner or controller will provide the requisite notification to relevant regulators and individuals. As a result of this framework and increasing scrutiny associated with breach events, businesses and their vendors now regularly engage in arm's-length contract negotiations to establish the scope and timing of breach reporting commitments in contracts and allocate the cyber risk in the event of a security breach suffered by the vendor.

Other than regulatory fines, there are two primary sources of costs and liabilities that result from data breaches: (1) costs incurred to remediate and recover from the incident, and (2) costs to defend third-party claims and potential liability resulting from those claims (including damages, non-compliance fines, civil penalties, assessments and settlements). The strategy for how an organisation should deal with these negotiations depends largely on their notification obligations under the breach laws. For example, organisations acting as data owners or controllers typically try to maximise liability protection, while entities acting as service providers or processors typically try to minimise their exposure in the event of a breach. Following the implementation of the GDPR in the European Union, the spectre of potentially significant regulatory fines resulting from data breaches is now often at the front and centre of contractual negotiations. While the security obligations of the GDPR apply directly to processors, controllers remain accountable for the data processed by their processors, and thus this shared regulatory risk must be allocated in the agreement.

Cyber insurance considerations are an important aspect of the vendor negotiation process as well, particularly if there are concerns regarding a vendor's solvency, such that an indemnification for data breaches may not itself be sufficient. It also may be important for ensuring that a vendor has sufficient insurance to stay in business while it processes the data owner's personal information, since large-scale security breaches can often result in millions of dollars in liability exposure for vendors. This number can grow exponentially if multiple corporate customers are affected by the breach.

Key considerations in messaging

With the uptick in breach notification laws around the globe, another key challenge facing organisations is the enhanced media scrutiny that companies now face in the wake of discovering a breach. Given the nature of today's media, social media and the blogosphere, organisations experiencing significant breaches often face a number of difficult decisions soon after discovering a breach, starting with balancing their knowledge of the facts (or lack thereof) with the need for a public statement. Security breaches are making their way into the public domain quicker and more commonly than ever before, attracting attention from the media, customers, regulators and plaintiffs' attorneys often early in the response process. In some cases, this can create a very difficult set of facts to manage without appropriate preparation.

Organisations that have developed their core public messaging simultaneously (e.g., an initial public statement in response to a leak, notices to affected individuals and media updates to address misinformation or reassure affected individuals) in anticipation of plausible data breach scenarios are in the best possible position when it comes to public messaging.

We have identified the core public messages typically necessary in the wake of a data breach and have provided a description of each.

Initial statement regarding the event

Organisations typically do not have much time to investigate a major data breach before the media learns of the incident. In response to an early media enquiry or report, organisations should be prepared to issue an initial statement either directly to the reporter who breaks the story or quickly after the publication of the first story covering the event. These holding statements should be general and describe the steps the company is taking in response to the situation. Organisations should avoid making definitive or speculative statements about the nature of the incident or scope of impact earlier in its response because the facts often change as the investigation progresses. A previous statement that includes misleading or false information about the breach could trigger the need for the organisation to later issue a correction or clarification.

Individual notification

After making an initial statement, organisations often face another difficult decision regarding when to update the public about their investigation, while also facing pressure to notify affected individuals. Notifying individuals can create the risk of discovering new or contradictory details about the incident, which then must be disclosed. An organisation's approach to this set of concerns depends largely on the particular circumstances and media coverage associated with the event, as well as the specific timing obligations they face. In preparing these notifications, organisations face the challenge of complying with their obligation to include certain legally required content while avoiding overly legalistic terms or alarming messages. Notifications to individuals generally should describe the key facts of the incident in plain and intelligible language, without using confusing legal jargon or including insignificant details.

Media responses

After disclosing an event to the public, organisations sometimes decide to provide additional communications to address misinformation or reassure affected individuals and investors – especially if the headlines following the breach event are critical of the company. For breaches that are not as severe, or do not attract substantial media attention, public disclosures regarding the breach after providing notification to affected individuals typically are limited.

Furthermore, beyond traditional media outlets, social media websites, such as Twitter, often attract an active community of privacy and cybersecurity advocates and reporters who not only provide timely updates about breaches, but also engage in online conversations about the breach event. It is increasingly important for organisations to monitor these sites to facilitate a quick response to any inaccurate information before that information is picked up and spread.

In drafting these public responses, it is important for the messaging to be consistent with earlier statements made about the incident. The responses also should avoid overstating the organisation's security practices or introducing false or misleading information about the breach that could later be used against the organisation in lawsuits or regulatory proceedings.

Conclusion

Given the ubiquity and inevitability of data breach events, organisations that are able to quickly identify, evaluate and remediate a breach are in a better position from a legal and public relations perspective than those who are slow to react. With the emergence of differing breach notification standards across the globe, notification for global organisations is becoming increasingly challenging. Differing contract requirements and statutory obligations, together with the fast-changing media environment and possibility of substantial fines associated with mishandling a breach, have created a perfect storm of data security concerns for organisations operating in a global setting. Preparing for this inevitable storm is critically important and organisations are focusing increasingly substantial resources on developing global data breach response procedures in an effort to ensure breach response efforts are as seamless as reasonably possible, under the circumstances, across the various interested business functions and geographies involved in the event. Those organisations that have a legal response procedure that seeks to address these complex issues in a manner that facilitates a thoughtful and nimble approach are optimally equipped to balance efficiently and effectively the legal, reputational, operational and financial risks arising from these multi-faceted events.

Appendix 1

About the Authors

Aaron P Simpson
Hunton Andrews Kurth LLP

Aaron Simpson is a partner with the global privacy and cybersecurity practice, resident in the firm's London and New York offices. Aaron's work ranges from advising clients on large-scale cybersecurity incidents to the development of cross-border data transfer solutions, compliance with existing and emerging data protection requirements in Europe, and negotiating data-driven commercial agreements. He has been recognised by *Chambers and Partners*, *Computerworld* and *The Legal 500* for his work on behalf of clients. Aaron also is a frequent speaker and has written and co-written numerous articles, book chapters and handbooks on privacy and cybersecurity issues.

Adam H Solomon
Hunton Andrews Kurth LLP

Adam Solomon is an associate with the global privacy and cybersecurity practice, resident in the firm's New York office. Adam assists clients in identifying, evaluating and managing global privacy and information security risks and compliance issues. He advises clients on all legal issues associated with information security programmes, cybersecurity incidents and electronic surveillance practices. He also assists clients with complex commercial contracting matters relating to privacy, data protection and information security issues.

Hunton Andrews Kurth LLP
30 St Mary Axe
London, EC3A 8EP
United Kingdom
Tel: +44 20 7220 5700
Fax: +44 20 7220 5772
asimpson@huntonak.com

200 Park Avenue
New York
NY 10166
United States
Tel: +1 212 309 1000
Fax: +1 212 309 1100
asolomon@huntonak.com

www.huntonak.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-223-7