

The Sedona Conference WG11 Brainstorming Group Outline – Incident Response Guide, Second Edition (October 2022)



The Sedona Conference Working Group 11 Brainstorming Group Outline - Incident Response Guide, Second Edition

I. INTRODUCTION

A. **Background and Questions for Annual Meeting Discussion:** The Data Security and Privacy Liability Working Group 11 (WG11) Steering Committee provided the following group objective to this Brainstorming Group (BG) and tasked us with submitting a final outline on October 14, 2022. We completed this initial draft to generate discussion and solicit feedback from the WG11 group at the Mid-Year Meeting to be held on November 2-3, 2022, in Cleveland, Ohio, and during a session at the WG6 Annual Meeting on January 11-12, 2023, in London, United Kingdom.

B. **The Objective of the Group:** The BG should evaluate the desirability of convening a drafting team to prepare a second edition of WG11's Incident Response Guide (IRG). Updates and additions for a second edition of the IRG that should be considered by the BG are:

- international incident response issues;
- emerging types of incidents such as ransomware; and
- updates reflecting key legislative changes.

C. **Questions for the Midyear Meeting and Annual Meeting:** Fundamentally, we are interested in suggestions/comments/reactions from the full WG11 on two issues: (1) whether developments in the laws in the United States and the world since January 2020 and the emergence of new types of cyber incidents warrant the appointment of a drafting team to write a second edition of the IRG and (2) if such an updated guide is warranted, what additional topics should be included as capable of consensus in moving the law forward in a reasoned and just way? This outline explores these issues as follows.

II. OVERVIEW OF PRIOR GUIDE AND ITS INTENDED AUDIENCE

A. WG11 published the first edition of the IRG in January 2020.

B. The goal of the IRG was to provide not only a high-level overview of the legal issues that should be addressed when an incident occurs, but also to provide practical guidance such that the IRG can be employed largely as a single-source reference to guide the user through the various legal and operational steps necessary to respond to an incident. The IRG addressed the foundational legal principles of breach notification requirements, principally by presenting those requirements grouped according to the types of obligations that U.S. jurisdictions typically impose, including subcategories for details such as the timing, content, and recipients for breach notifications.

C. The IRG is divided into the following parts:

- Pre-Incident Planning
- The Incident Response Plan

- Executing the Incident Response Plan
- Key Collateral Issues
- Basic Notification Issues
- After Action Review

D. The IRG also provides sample notification letters that could be used according to different jurisdictional requirements, as well as a Model Incident Response Plan.

E. The target audience for the IRG is small to medium-sized organizations, which typically do not have unlimited resources to devote to incident response.

III. WHETHER A DRAFTING TEAM SHOULD BE CONVENED TO PREPARE A SECOND EDITION

A. Overview of our recommendation:

1. The BG believes it is worth forming a drafting team to prepare a second edition of the IRG.

Most notably, there have been significant developments in incident response since the IRG was first published. These developments, described in detail below, create a need for an updated IRG that addresses the following: (1) international incident response, especially because of the enactment of breach notification laws in foreign jurisdictions; (2) emerging types of incidents such as ransomware and business email compromise that continue to impact organizations large and small; and (3) key legislative changes to U.S. laws that impact incident response procedures.

2. General Drafting considerations/questions

To what extent should we seek to operate within the confines/organization of the existing draft? For example, the discussion of incident types currently sits largely within a discussion about engaging law enforcement. Should ransomware and BEC be added to that discussion, or should we break that out as a larger, standalone discussion about incident types?

B. Emerging Types of Incidents Should be Included in a Second Edition of the IRG

1. **Scope** – Consider whether to update the IRG to address ransomware, business email compromise (BEC), and other types of incidents.
2. **Recommendation** – We recommend updating the IRG as outlined below.
3. **Incidents to include in revision**

a. Ransomware

- i. Evolution of ransomware (e.g., double- and triple-extortion, targeting executives, etc.)
- ii. Issues implicated – business interruption, compromise of personally identifiable information (“PII”) or protected health information (“PHI”), adverse publicity, notification obligations, regulatory compliance (e.g., Office of Foreign Assets Control), etc.
- iii. Cross-reference to forthcoming Sedona paper regarding ransomware +payments

b. Business Email Compromise

Statistics showing prevalence of BEC

Issues implicated – loss of money/wire diversion, compromise of PII/PHI, adverse publicity, notification obligations, etc.

- c. **Other types of incidents** (e.g., third-party breaches) Breaches of sub-contractors and companies engaged in mergers and acquisitions, targets in particular.

4. Other comments

While we recommend that the IRG contain a discussion of the types of incidents, we recommend keeping the discussion general in nature and focusing on the fact that the types of attacks have and continue to evolve. Attempting to catalog all incident types or provide technical details poses a risk that the IRG could become “outdated” quickly.

5. Suggestions as to where to update the IRG

Refer to ransomware in II.A. given importance of data mapping, back-ups, etc.

- i. Add discussion to V.A. for ransomware, BEC, etc. and considerations for engaging law enforcement for those types of incidents. This discussion could be in an expanded list of incident types (see pages 153-57) of existing IRG

1. For ransomware, note OFAC guidance for interactions with law enforcement.
2. For BEC, explain the importance of prompt communication with law enforcement if trying to recover money, especially overseas.
3. Consider more robust discussion of notice to insurers in V.B. (page 157) and discussion of insurance considerations regarding the availability of coverage for ransom payments.
4. Consider more robust discussion of engaging outside vendors in V.E. (pages 161-63); e.g., ransom negotiators, vendors for OFAC due diligence
5. Coordinate any revisions to Notification section (VI.) with that drafting sub-group (pages 170-234)
6. Discuss notification considerations unique to ransomware (e.g., HIPAA).
7. Discuss data mining and possible notification obligations stemming from BEC.
8. Discuss notification obligations stemming from contracts, court orders, sources other than statutes and regulations.
9. Update Appendix A (Model Incident Response Plan) to reference ransomware, BEC, etc., in types of incidents (page 240) and elsewhere as needed
10. Update Appendix F (GLBA and HIPAA) as needed (pages 259-62)
11. Add discussion of the need to consider whether a ransom payment is prohibited by law, for example, if a threat actor is listed on a sanctions list. Identify that the legality of ransom payments is jurisdiction-specific.

6. Suggestions as to how to keep current to reflect new threats

- a. Join CISA alerts
- b. Join ISACs
- c. Join industry groups known for information sharing.

C. Key Legislative Changes Should Be Included in the Second Edition of the IRG

1. Scope – Update the IRG to address changes in state, federal, international, and commercial notification requirements, recognizing that international will be addressed by another subgroup, but presumably integrated into the existing structure.

2. Changes to incorporate

- a. State law
 - i. Definitions expanded to cover broader categories
 - 1. Protected information
 - 2. Protected individuals
 - ii. Changes in notification deadlines
 - 1. Individuals
 - 2. Regulatory authorities
 - iii. Miscellaneous – e.g., safe harbor for Ohio, Utah
 - iv. Judicial interpretations of note
- b. Federal law
 - i. Prudential regulatory
 - 1. Materiality
 - 2. Timing trigger
 - ii. Critical Infrastructure
 - 1. Materiality
 - 2. Timing trigger
 - 3. Anticipated scope (predictive at best)
- c. Commercial requirements
 - i. Partners
 - ii. Vendors
 - iii. Memorializing and accessing when systems inoperable
- d. Changes in Cyber Insurance
 - i. More requirements to get insured
 - ii. Increased cost and lower caps

iii. Self Insurance

3. How best to update the IRG

- a. Retain existing structure and supplement to the extent possible
- b. Add new sections/move topics as needed

4. Update each key section

- a. Has a ‘breach’ occurred?
 - i. Is PII implicated?
 - ii. Access or acquisition
- b. Exceptions to Breach
 - i. Encryption
 - ii. No risk of harm¹
 - iii. Employee good faith (any changes?)
- d. Who must be notified?
- e. When is notification required?
 - i. Aggressive deadlines from regulators/Attorney’s General/SA’s
 - 1. May not automatically trigger individual notifications
- f. Cross-triggers
 - i. Other regulators
 - ii. Individuals
 - iii. Credit monitoring agencies (still relevant?)

¹Because the nature of data breaches has evolved to include an increased scope of PII, the scope of harm has likewise evolved. Accordingly, the next step in determining whether notification of a security incident is required involves performing a “risk of harm” analysis. Put in the simplest of terms: if an individual is likely not to experience harm as a result of a Security Breach, then providing notice to that individual is unnecessary. The vast majority of state data breach notification laws require some analysis by the impacted PII Controller of the risk of harm to the individual associated with the PII in question by reason of the event in question before a notification requirement is triggered. The standard for determining whether a sufficient risk of harm exists to require notification varies across those states, however, and uniformity is necessary to eliminate confusion.

The Drafting Team notes that the risk of harm assessment generated significant discussion within the Team and seeks guidance from WG11 on the applicable scope of this discussion in updating the Incident Response Guide. This statutory “risk of harm” analysis for breach notification is related to but very distinct from the question of whether “concrete, particularized harm” or “intangible” injury exists—including the “risk” of injury—that is central to whether plaintiffs have standing to sue over a data breach and whether their claims are viable. The “risk of harm” analysis for statutory data breach notification purposes presents different concerns from the “injury” requirement for Article III standing. Accordingly, this commentary refers only to “risk of harm” in statutory construction and is not intended to provide any analysis concerning venue or jurisdiction in litigation.

5. Include contextual discussion of interplay among reporting obligations

- a. *How will more aggressive international notification obligations impact U.S. notification scheme?*
- b. Interplay among exceptions
 - i. Risk of harm examples
 - 1. Recap summary
 - 2. Florida example: notify law enforcement
 - 3. HIPAA standards and procedures
 - 4. Judicial interpretations (e.g., Uber bug bounty failed recharacterization)
 - 5. California/Others as outliers
- c. “Non-public” notifications to Supervisory Authorities
 - i. Prudential Regulators (the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and the Federal Reserve Board)
 - ii. CISA
 - iii. NYDFS
 - iv. GDPR Article 33
- d. Interpreting and executing cross-notification triggers
- e. Other considerations
 - i. Precautionary trading blackouts
 - ii. SEC considerations

6. Highlight proactive assessment and planning as key in an IR Plan

- a. Striking the balance among mandatory notifications, discretionary notifications, protective/precautionary notifications
- b. Guidance on frequency for updating the IR Plan
- c. Memorializing the basis for the decisional process

7. How does Sedona keep up?²

- a. Identifying priority regulations/topics for updates
- b. Timing for updates - ad hoc or regular intervals

² The Drafting Team notes that keeping up with all applicable laws and regulations across the globe generated significant discussion within the Team and seeks guidance from WG11 on processes for reasonable updates.

D. International Incident Response Procedures Should be Included in the IRG

1. Scope

- a. Incident response has developed significantly since the first draft of the IRG. The majority of incidents we support have an international element, whether it be through an outsourced provider or local offices. While we recognize that the IRG is not a globally comprehensive guide, we believe the new draft of the IRG should reflect the key issues and material obligations arising in key economic jurisdictions.
- b. When the IRG was first drafted, notwithstanding the fact that the US has had reporting obligations for almost 20 years, since 2018 the EU's GDPR has been seen as the golden standard for reporting obligations. The as it set a 72-hour reporting timeline was also one of the shortest. Since then there have been developments in other jurisdictions and EU laws that significantly reduce these timelines, for example, India's proposed reporting requirement of 8 hours and Russia's of 48 hours. Developments such as these need to be captured in the IRG.
- c. For the assessment of any incident, the risk of harm analysis is critical and is treated very differently in the U.S. than in international territories. A primer on key highlights outside the US should be included in the IRG (e.g., the EDPB Guidelines on breach response and developments in implementation of the GDPR).
- d. A brief outline on when international companies are subject to the reporting requirements under the GDPR is also advisable..

2. **Recommendation** – While we acknowledge the target audience of the IRG, in an increasingly digital and globally-entwined economy, this audience is more likely than not to have some form of outsourcing to another country or targeted advertising of individuals outside the US. Therefore, some thematic ideas should be discussed so that organizations are aware of key international issues and material differences to local laws at the outset of the incident. The IRG must convey the message that the requirements of international jurisdictions should not be an afterthought in breach response.

3. Issues to consider in the revised IRG

- a. The IRG lends itself well to amendments as it already addresses international issues, for example, as references to the GDPR and the EU's position already appear in many sections, for example:
 - i. Discussion of European Cybercrime Centre (page 155)
 - ii. Local Pg 181ff – risk of harm analysis
 - iii. Timing of notification “without undue delay” (page 205)
 - iv. Timing of notification (page 213ff)

- v. Other issues that could be considered in the revised IRG include:
 - vi. Issues relevant to local / international counsel could also be addressed in conjunction with the vendor selection section at pages 161-162.
 - vii. General commentary on the availability of credit monitoring outside the US could be added at page 168.
 - b. Thematic issues can be discussed within section VI that can be applied across a number of international jurisdictions outside the EU, such as:
 - i. Notification - Expansion of the information on notification thresholds and risk of harm analysis to cover key economic territories and jurisdictions with unusual legal requirements or processes (e.g., Turkey makes all notifications public at the point of reporting; Alberta, Canada's Privacy Commissioner takes the view that virtually any incident gives rise to real risk of significant harm, triggering a notification obligation).
 - ii. Reporting deadlines and notification deadlines.
 - iii. Notification methods and content, e.g., some jurisdictions require local language.
 - iv. Key focuses of regulators and current investigation and enforcement trends both in the EU and in key jurisdictions outside the EU can be considered, for example:
 - 1. Appointment of a DPO / EU Rep / DP Rep;
 - 2. Scale/severity of an incident;
 - 3. Notification timelines following an incident; and
 - 4. Remedial steps to be taken following an incident.
 - c. It may also be useful to set out some of the key points arising from the EDPB Guidelines, which appear to set the tone for many international legislative frameworks, including U.S. state laws.

IV. PROPOSED DRAFTING TEAM

Possible Drafters:

1. Outside US counsel representing organizations who provide notice of a breach
2. Outside International counsel representing organizations who provide notice of a breach
3. In-house counsel
4. Non-lawyer corporate/government officer with data security responsibilities (e.g., Chief Information Security Officer)
5. Consumer protection regulator
6. Professor
7. Cybersecurity consultant/investigator
8. Cyber insurance professional

This confidential outline of The Sedona Conference Working Group 11 on Data Security and Privacy Liability is not for publication or distribution to anyone who is not a member of Working Group 11 without prior written permission. Comments and suggested edits to this document are welcome by email to comments@sedonaconference.org no later than December 5, 2022.

9. EDPB Representative (or those who routinely deal with EDPB)