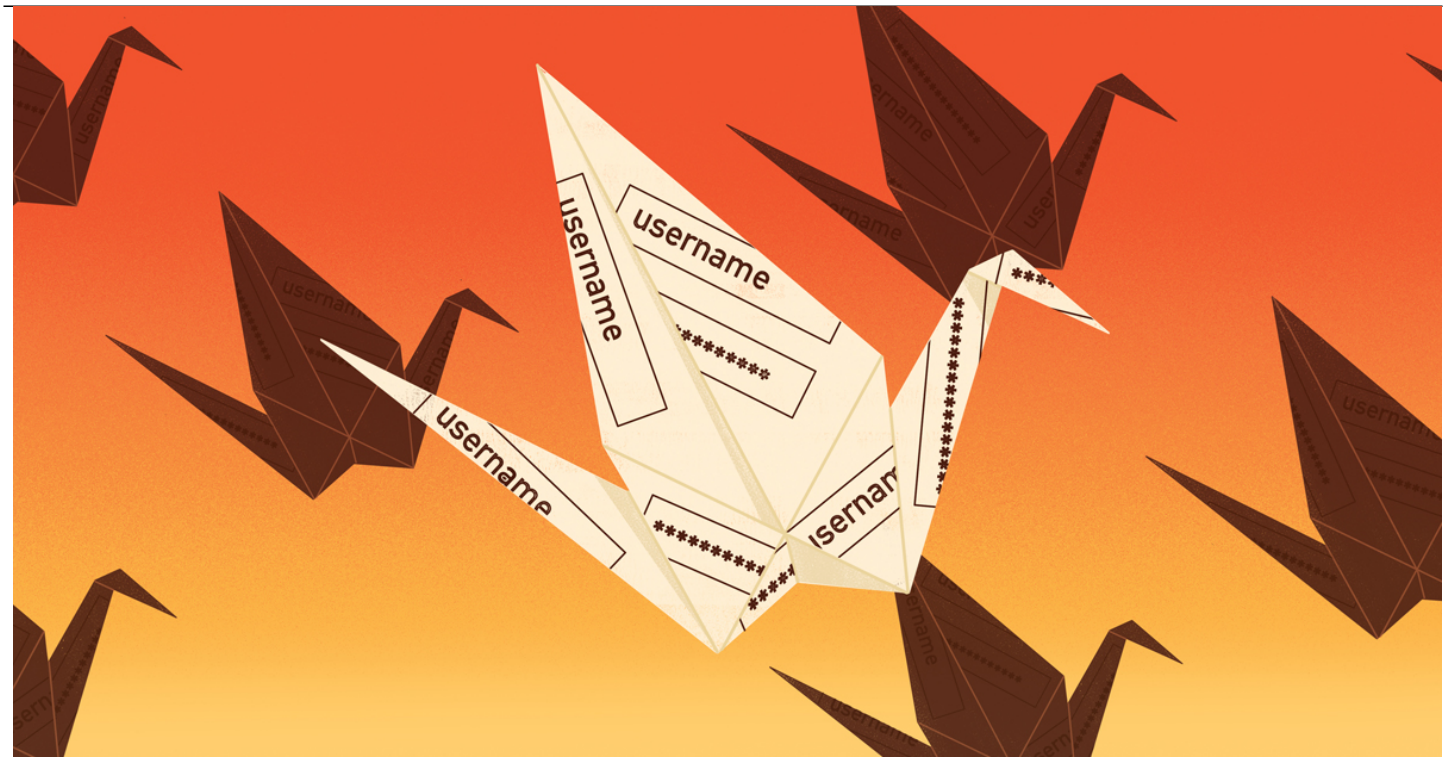
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Data Breach! A Playbook for The First 72 Hours

Law Department Management

Technology, Privacy, and eCommerce



[Request reuse permissions]

Original banner artwork by Chris Gash

Cheat Sheet

- **First 6 hours.** A clearly established chain of command and effective process and governance is key first step.
- **First 12 hours.** Keep an open mind as everything can change as more data and evidence emerges. But be ready to act quickly.
- **First 24-36 hours.** Communicate the clearest picture you have as notification laws and requirements typically go into effect during this timeframe.
- **And ongoing.** While the first 36 hours are critical, there may be litigation costs, regulatory fine risks, legal, consultant and advisor fees, and lost customer revenues that will be key factors in prioritizing next actions to manage the incident.

The first 72 hours is the most critical time period for the necessary actions after discovery of any cyber-attack that may involve personal data/personally identifiable information (PII) that is stored or processed by your company. How ready your business is for such an incident and the steps and decisions that are made in this initial time frame are critical to how quickly the business can recover operationally and reputationally from the attack.

The following is suggested as a practical list or “playbook” for necessary actions for an in-house legal team and executive management. This is written mainly from a GDPR EU/EEA and UK perspective but has global applicability; it assumes that industry-standard security and data compliance processes and policies are already in place for the affected entity or demonstrates why they should be.

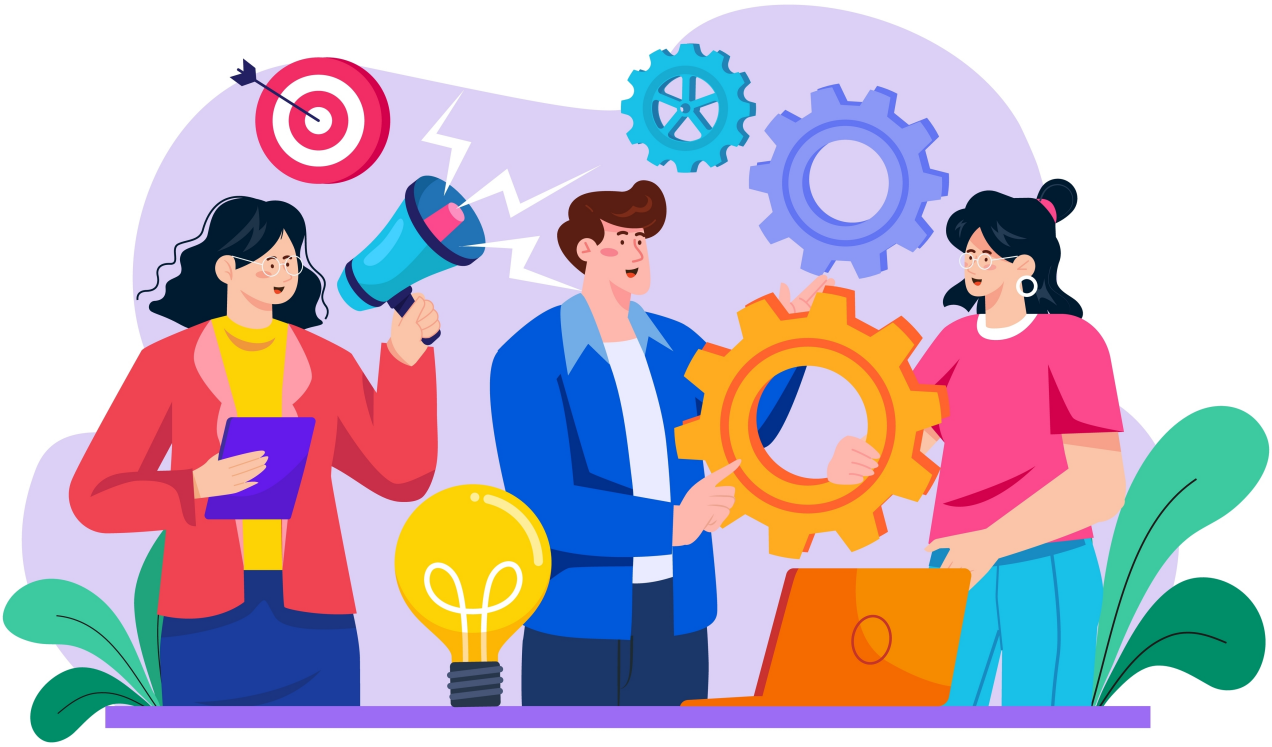
The first 6 hours

The **overarching initial requirement** is to implement process and governance.

“Chain of command — build the machine”

This means confirming **who leads what**, the response committee/team structure, roles and responsibilities, meeting cadence, and communication lines. Your existing policies and written procedures should have considered and will support this (and hopefully have been road-tested in table-top exercises or mock data breach training).

During this initial period of disruption, policies/procedures can be forgotten or neglected as a crisis unfolds. Legal can play a key role in helping guide the business in **rapid creation of a functional, adequately skilled response team**. This is critical to ensuring that resources are deployed and focused on their most valuable tasks and that efficient information-sharing can support fundamental decision-making taking place during this period.



During the first 6 hours of a data breach, confirm who leads what. hoangpts / *Shutterstock.com*

Committees, reporting, and meeting minutes

A core team of decision-makers is needed to receive regular status reporting from across a range of workstreams (CISO, forensic investigators, account managers, litigation teams etc). **Immediately start minuting this and all meetings from the get-go.** This is a vital record of your response, the key decisions made (and their rationale), and loss mitigation.

This also presents a picture of good governance and mature response planning should a regulator challenge. You will need resources for tracking meetings, attendees, and decisions made. This is challenging as there can be many parallel meetings, sometimes non-stop, for some days. Get those resources ASAP, which may mean re-deploying resources from other projects for a short, critical period.

> Legal can play a key role in helping guide the business in rapid creation of a functional, adequately skilled response team.

Policies — follow them

The question will come up later: **Did you follow your company's crisis incident response policies?** Record this — and if deviating, make sure that this is also recorded with the explanation. If the policies say that the head of security will chair meetings, make sure that occurs. It's a detail that will show that you were on top of both the big picture and the details.

Also, well-prepared policies will have pre-considered many of the key issues and will be grappled with as part of the response; don't throw out that preparation and learning by ignoring the policy when an incident occurs.

The first 12 hours

"Exercise caution — assume the worst (even if that makes you unpopular)"

At this stage a view of the facts surrounding the adverse event may start to emerge. It is advisable to take a cautious view regarding “facts” at this early stage — **even a cynical view as “devil’s advocate”** — because everything can change as more data and evidence emerges. These are complex investigations typically without "perfect picture" of all threat actor activity. Be wary of “good news.” If needed, develop hypotheses and test these with an open mind with the technical experts.

- **Is the event ongoing?**
- **Is it contained?**
- **Is the threat actor still within the business environment?**
- **Is a view of accessed / exported data emerging?**
- **Is the cause or access-point known?**
- **Is the scope of compromised assets fully understood?**
- **What is the chain of evidence?**
- **Do we have indicators of external third parties becoming aware?**

Answers to these questions can change as technical and forensic teams continue their work. Allow some time for data/evidence to emerge, and for technical and forensic teams to advance their analysis outside their reporting updates and meeting attendance. Continually test for levels of confidence in any interim conclusions being reached in this early stage.

Because everything can change as more data and evidence emerges.

Engage the necessary suppliers; consider legal privilege

This needs early consideration. Engaging external lawyers can support a high level of legal professional privilege. You may also want to engage specialist cyber-investigations or security consultants — the external law firm could engage them to potentially have a stronger privilege position if loss or harm is anticipated.

It is in your best interest to have cyber-security specialists in terms of support during the preparation planning stage. Net Vector / *Shutterstock.com*

It can be valuable to have cybersecurity specialist consultants on stand-by, already under contract, and ready to be engaged by the company or its representatives — this will avoid any rush to engage these suppliers. As part of preparation planning, having these third parties identified (and ideally engaged) is key, e.g., crisis management consultants and contact center providers.

Senior management input and reporting

Prepare or commence senior management reporting. Ensure that reports confirm the application of the company's policies, and any necessary deviations. Request board feedback and direction where appropriate — especially if existing policies do not cover your situation (e.g., ransomware attack response?).

Credit card issuer notification

If credit card data was affected — even if encrypted and without CVC/CVV numbers — call the largest credit card issuers to alert them. They may commence fraud monitoring as a loss mitigation step. Their security hotlines might only ask that you leave a message — but do that and then send an email (they will call you back).

Insurer notification

Consider your insurance policies and the required insurer notifications. You will need to understand the notification process and initial data needed. Rigorous expenses monitoring will be expected by insurers. Also consider privilege issues when disclosing key reports or updates to the insurer.

Check out this recorded webcast, "Data Breach - A 'First Response' Legal Playbook" with *Docket* authors Stephen H. Baird and Simon Elliott.

The first 24-36 hours

The chain of command is in place, it is receiving reports, and the roles and functions are established. By now an evidence-based view of the actual situation may be emerging.

"Time for wider notifications”

Notifications are required under relevant laws. Regulators often require notification of reasonable suspicion of data breach, as well as actual known data breaches. They often encourage initial notifications to put them on notice in case they need to act to support.

You should aim for communicating the **clearest picture possible**, in a way that can be substantiated later. This can be difficult as often your teams will not know all background — but this is not an excuse for not notifying the necessary parties.

Be certain to notify your team and all necessary parties of the data breach with as much background knowledge as possible. phoelixDE / *Shutterstock.com*

Customer notification

You should be preparing to advise any affected customers now. In a B2B context, phone calls and then formal letters to corporate customers may be appropriate. **This will require relevant staff to step in to own the communication process to ensure maximum clarity and effectiveness.** Customers will typically understand if initial notifications are not complete, when you make it clear that investigation is ongoing. If B2B, you will typically need to offer to send the customer a copy of any egressed data securely. Be ready for a wave of follow-up questions and requests for further information. Key accounts may need careful management; but preparing FAQs and centralized messages will support this.

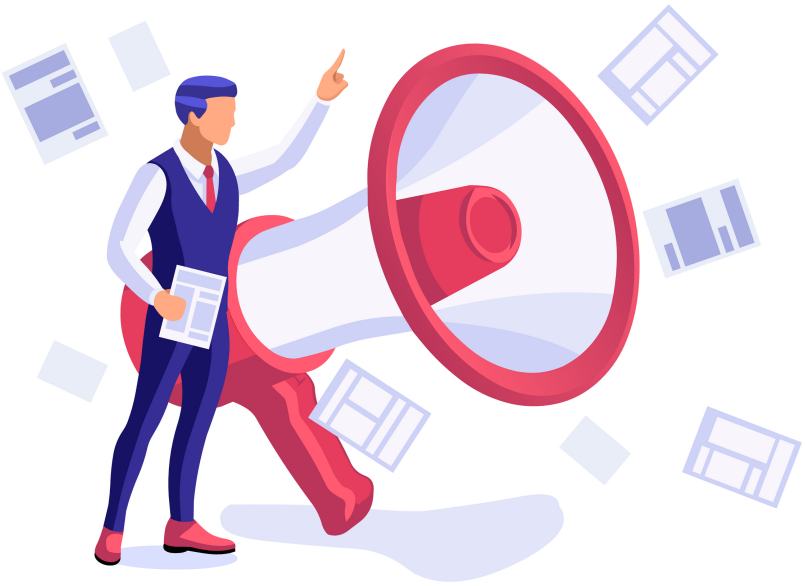
As noted above, the technical teams' assessment of affected volumes of personal data/PII may change as the investigation continues, but that is usually not a valid reason to delay action for an extended period after knowledge of an adverse event (or reasonable suspicion of one) is established. Do not use the fact that you may be a B2B subcontractor/service provider ("data processor" in EU GDPR terminology) as a reason to delay the necessary action — in the EU/EEA, data processors need to act swiftly, as well as data controllers.

Be ready for a wave of follow-up questions and requests for further information.

Government agency/regulator notification

Consider the necessary regulatory notifications. Even as a B2B sub-processor/contractor, in some jurisdictions it is mandatory to report incidents relating to personal data/PII to data privacy regulators. If you have customers based in these countries, you may need local external law firm support for this process. Consider also law enforcement reporting if criminal activity is suspected (cyber-crime divisions of law enforcement agencies), and any relevant critical infrastructure monitoring agencies requiring notification of cybersecurity incidents.

ACC'S resource library has sample data breach notification policies for ACC members.



A communications strategy will need to be implemented to address questions and concerns. aurielaki / *Shutterstock.com*

Publicity

The public relations/communications/marketing team will need to prepare a reactive statement and begin to consider proactive website and public communications strategy. **Note that "crisis communications" is a particular discipline within communications — your team may need**

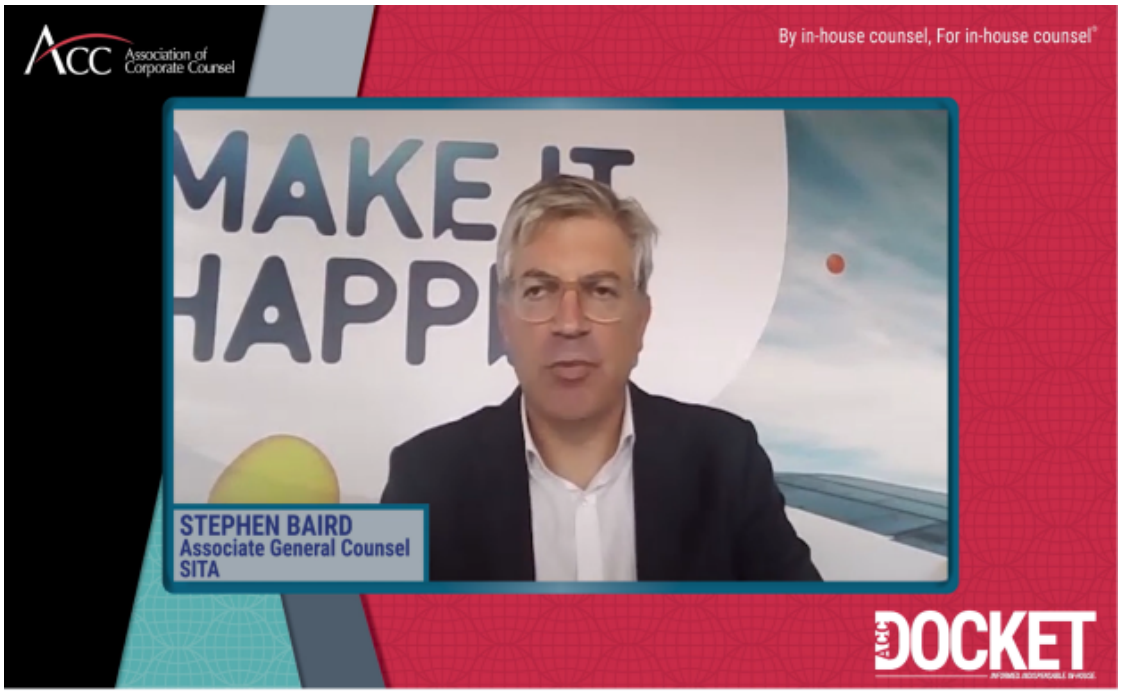
specialist external “crisis comms” support. Be aware that journalists requesting comment often provide only a short window of time (perhaps only one hour) before going to press. Make sure ownership here is clear. Consider transparent internal staff messages and updates as well.

“How much will this cost?”

Cost

Later, senior management are likely to request a loss estimate. For large personal data/PII incidents this can be difficult because much depends on uncontrollable factors — such as litigation costs, regulatory fines, legal, consultant, and advisor fees, lost customer revenues, and so on. It’s sensible to ensure any estimates are clearly noted as preliminary and management understands the scope for later variations in the estimates.

If the data incident that you are managing is serious, ensuring that the first hours are handled in the most expedient way will support future loss mitigation and damage control.



3 Minutes with an ACC *Docket* Author

Check out this clip from *Docket* author Stephen Baird as he comments on his most recent article, "Data Breach! A Playbook for the First 72 Hours."

Stephen H. Baird

Associate General Counsel

SITA

Stephen H. Baird is an associate general counsel at SITA, the world's leading specialist in air transport communications and information technology. SITA serves over 200 countries and territories and is headquartered in Belgium and Switzerland. Baird graduated from the University of Western Australia's Law School and was a Federal Court of Australia Judge's Associate (clerk) before working in private practice for several years. He has worked as counsel for SITA for 19 years, leading on product technology, data and trade law matters, and is currently based in Geneva, Switzerland. Follow him on LinkedIn.

Simon Elliott

Partner

Dentons

Simon Elliott is a partner at the law firm Dentons and leads its market-leading UKIME Data Privacy and Cyber Security group. He has 15 years plus experience as an expert advising clients on the full range of data privacy and cyber matters including leading large-scale global projects designing and implementing global privacy frameworks and strategies as well as supporting on the operationalization of privacy programs within organizations. Elliott also regularly assists major global multi-nationals and UK businesses with regulatory investigations and enforcement actions by privacy regulators, supports on the increasing flow of data protection litigation and media enquiries focusing on privacy practices. Elliott is identified as a "Next Generation Partner" by The Legal 500 for data protection, privacy and cybersecurity and is a Ranked Lawyer in Chambers for "Data Protection & Information Law".