



CRISIS HANDBOOK

A Desktop Investigations Guide



ABOUT CROWELL & MORING

Crowell & Moring is the first stop for hundreds of multinational corporations, closely held businesses, boards of directors, special committees, partnerships, and executives facing a crisis. Clients across the world trust us to resolve these high-stakes matters effectively and efficiently because we have a proven track record. Our team has successfully managed and defended a broad range of sensitive investigations—whether company initiated or involving federal prosecutors, enforcement agencies, grand juries, inspectors general, Congress, or state and local prosecutors.

Repeatedly named to the *Global Investigations Review's* “**GIR 100**” and ranked by *Chambers* for “**Corporate Crime**,” our lawyers represent clients in matters spanning more than 80 countries and six continents.

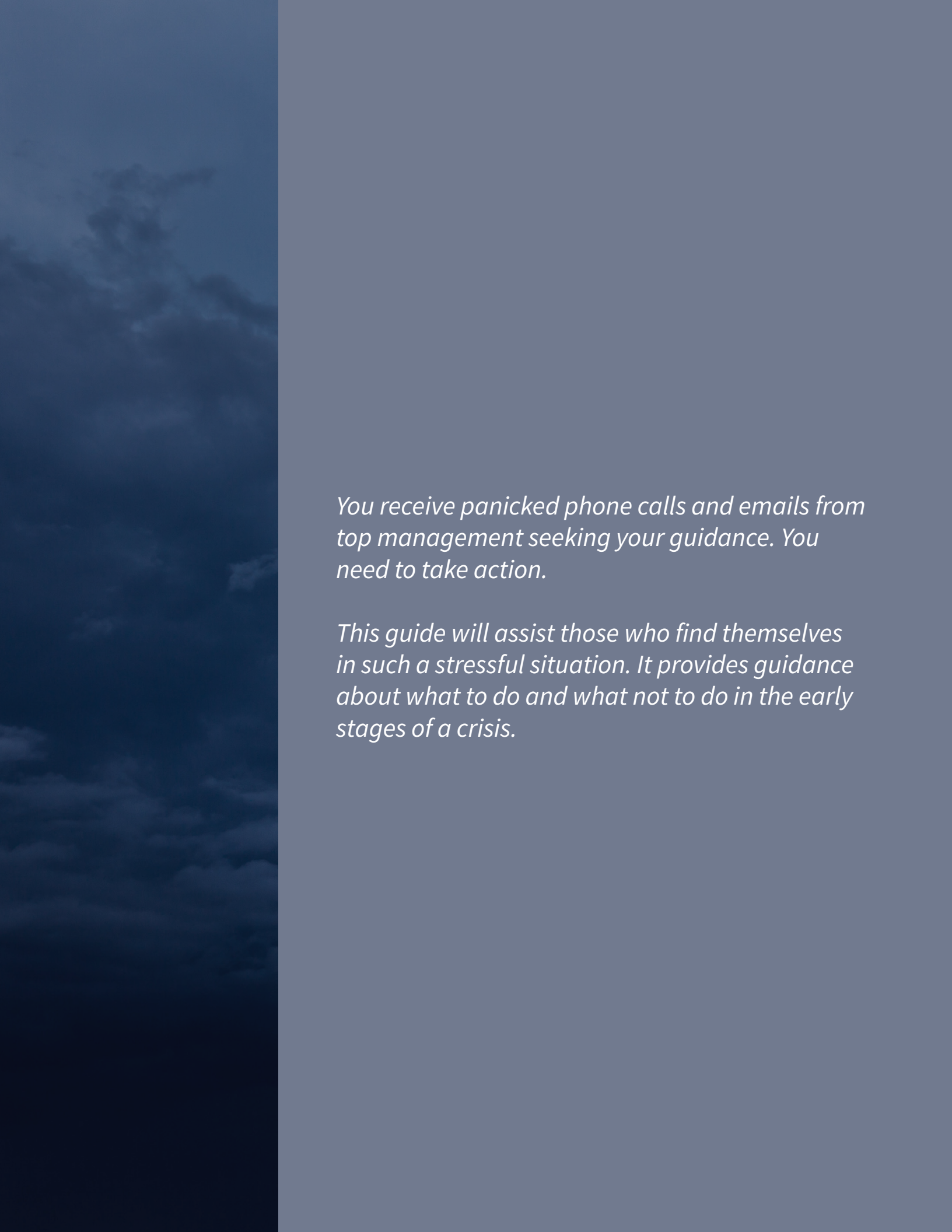
Our investigations team includes highly experienced white collar and regulatory enforcement attorneys across the globe. We have the rare blend of insight, experience, and judgment that only a team of lifelong defense lawyers, former prosecutors, enforcement attorneys, and agency officials can bring to the table. Many of our attorneys served at high levels within the:

- U.S. Department of Justice
- Securities and Exchange Commission
- Federal Bureau of Investigation
- National Intelligence Community
- Office of Foreign Assets Control
- Financial Crimes Enforcement Network
- Department of Homeland Security
- U.S. Congress

Learn more about Crowell at crowell.com.

TABLE OF CONTENTS

When Crisis Strikes	1
Internal Investigations—Goals	3
Maintaining Attorney-Client Privilege	4
Search Warrants.....	5
Search Checklist	6
Detailed Guidance	7
Government Subpoenas/Inquiries.....	10
Preservation Checklist.....	11
Detailed Guidance	12
Other Crisis.....	14
Samples	16
Search Warrant Notice to Employees	17
Preservation Notice	18
Upjohn Advisory	21
In-House CLE Offerings	22
Nuts and Bolts: Conducting an Internal Investigation	22
Attorney-Client Privilege: Fundamentals and Best Practices.....	22
Protections and Pitfalls Concerning Cross-Border Privilege Claims	22
Visit Us Online	23



You receive panicked phone calls and emails from top management seeking your guidance. You need to take action.

This guide will assist those who find themselves in such a stressful situation. It provides guidance about what to do and what not to do in the early stages of a crisis.

When Crisis Strikes

Crisis hits in many forms:

Law enforcement agents execute a **search warrant** at your company's offices.

FBI agents show up to interview employees.

A **news reporter** calls with questions about alleged payments to a government official.

A **whistleblower** provides confidential information and documents to government agents.

Your chief information security officer discovers a **ransomware attack**.

A federal agent serves you with a **grand jury subpoena**.

The SEC contacts your company and serves a **document preservation notice**.

An employee is **seriously injured** at work.

U.S. Customs seizes your property at the port.

A company executive is accused of **personal misconduct**.



Critical First Steps

Internal investigations are often the first step to assess—and help mitigate—legal exposure. Failing to conduct one properly could inflict further harm on your company.

This handbook starts with the typical goals of an internal investigation and provides guidance on protecting legal privileges. It then covers two common crisis scenarios: search warrants and government subpoenas/inquiries, including “do this” and “not this” checklists followed by detailed guidance.

We also provide general guidance on several other types of crisis scenarios, as well as samples for use during an investigation.

Internal Investigations—Goals

Ten Common Goals

1. Understand the facts
2. Understand the root cause(s)
3. Maintain privilege
4. Preserve relevant evidence
5. Assess criminal, regulatory, and civil exposure
6. Remediate/mitigate
7. Minimize business disruption
8. Determine disclosure obligations
9. Avoid criminal referral, prosecution, and civil enforcement action
10. Minimize parallel civil litigation risk

Detailed Guidance

- **Understand the facts.** Learn the facts surrounding the alleged misconduct and lay the foundation for an appropriate and accurate inquiry.
- **Understand the root cause(s).** Pinpoint the core reason behind an incident—not just “how” but “why” it occurred.
- **Maintain privilege.** Preserve confidentiality and legal protections to maintain options and minimize damage from disclosing protected information to a third party.
- **Preserve relevant evidence.** Identify all sources of relevant evidence and implement back-end holds on relevant data systems and employee accounts. Issue a Preservation Notice ([sample here](#)) to identified custodians as soon as possible.
- **Assess criminal, regulatory, and civil exposure.** Systematically evaluate the potential risks and vulnerabilities based on alleged conduct.
- **Remediate/mitigate.** Formulate strategies and establish a formal, documented process to ensure that corrective actions (if any) are identified, implemented, and verified.
- **Minimize business disruption.** Use a designated team to facilitate data collection and interview scheduling to avoid productivity interruptions.
- **Determine disclosure obligations.** Assess and comply with disclosure obligations—which can run to investors, lenders, auditors, insurers, and business partners—to minimize future disputes and maintain transparency.
- **Avoid criminal referral, prosecution, and civil enforcement action.** Develop strategies that decrease the risk of triggering criminal referrals, prosecutions, and civil enforcement actions.
- **Minimize parallel civil litigation risk.** Develop a comprehensive strategy to mitigate the risk of and address the procedural and substantive challenges associated with parallel civil proceedings.

Maintaining Attorney-Client Privilege

What is Attorney-Client Privilege?

The attorney-client communications privilege applies to confidential communications between employees and counsel for the company for the purpose of assessing legal issues or providing legal advice to the company. Facts are not privileged, but the legal analysis of and conclusions drawn from facts are protected. The privilege belongs to the company, not to any individual officer or employee.

Likewise, the work product of investigations in anticipation of litigation, broadly defined, is generally protected.

To maintain privilege, always:

- Clearly mark privileged communications and work product.
- Document that the investigation's purpose is to provide legal advice to the company, and, where applicable, that it is being conducted in anticipation of litigation.
- Have counsel conduct the investigation or, at a minimum, actively direct non-attorneys conducting the investigation with written instructions and ongoing oversight.
- Take extra precautions in non-U.S. jurisdictions, where, for example, attorney-client privilege does not always extend to in-house counsel.

Employee Interviews

Upjohn Advisory: To maintain and protect the company's privilege over the investigation, counsel must make clear to interviewed employees that the interview is being conducted so that counsel can provide legal advice to the company. Always inform the employee that:

- You represent the company, not the employee.
- You are gathering information to provide legal advice to the company.
- The interview is confidential and privileged.
- The company alone will decide whether to waive or assert the privilege.
- The employee should not discuss the substance of the interview with others to avoid an inadvertent waiver.

Memorialize the Interview: Prepare a written memo of the interview. Note that counsel provided an Upjohn advisory and that the employee acknowledged it. Also note that it's not a transcription and contains counsel's mental impressions. A sample Upjohn advisory is included in this handbook.

Search Warrants

Be Prepared for a Search

It's alarming when armed law enforcement shows up brandishing a search warrant. Here's how to prepare for the worst in advance:

- Clearly mark privileged material and maintain it separately from non-privileged material.
- Maintain copies of essential business records off premises (including records stored on personal computers).
- Train at least one lawyer at each company facility on the proper response to a search warrant. For facilities where there is no lawyer, provide management with a point of contact in the event of a search.
- Identify experienced white-collar counsel before the need arises, and distribute counsel's contact information to key personnel.
- Develop a plan for closing the facility in case of a search.

Search Checklist

DO This

- ✓ Immediately contact experienced, external white-collar counsel.
- ✓ Identify and meet with the lead agent as soon as possible.
- ✓ Obtain and review the search warrant.
- ✓ Determine whether agents are detaining employees.
- ✓ Advise employees of their rights in the event the government attempts to interview them.
- ✓ Consider sending employees home.
- ✓ Object to any review or seizure of privileged materials, including legal communications.
- ✓ Make a record of events as they unfold.
- ✓ Ask to be present when the agents make an inventory of the property to be seized.
- ✓ Make your own inventory of the seized property.
- ✓ Ask for copies of seized electronic media.
- ✓ Ask for split samples (e.g., in environmental matters).
- ✓ Advise the lead agent of any classified data that exists.
- ✓ Advise employees not to discuss the search with others, except legal counsel.

NOT This

- ✗ Do not attempt to prevent the search from taking place.
- ✗ Do not obstruct the agents executing the warrant.
- ✗ Do not remove or destroy documents to prevent their seizure.
- ✗ Do not consent or otherwise give your permission to search any area or to seize any property.
- ✗ Do not instruct employees not to speak with agents (but advise them of their rights, including the right to/not to speak with agents).
- ✗ Do not volunteer substantive information.

Detailed Guidance

DO This

- ✓ **Immediately contact experienced, external white-collar counsel.**
- ✓ **Identify and meet with the lead agent as soon as possible.** Obtain the business cards, or at least the names and affiliations, of the agents involved in the search, as well as the name and contact information of the prosecutor responsible for execution of the warrant. Ask the lead agent for information concerning the status of the company (e.g., witness, subject, or target of the investigation) and the nature of the allegations being investigated. Ask whether any employees have been or are being interviewed, and, if so, request that legal counsel be present at any such interviews. Avoid discussing the factual basis of the investigation before consulting with counsel.
- ✓ **Obtain and review the search warrant.** Law enforcement is required to provide a copy of the warrant. Request one. Review the warrant as soon as possible to gauge whether the search is being limited to the physical areas and items specified in the warrant. General searches and “exploratory rummaging” are prohibited. Do not obstruct the agents if you feel the search is outside the scope of the warrant. Instead, if possible, make the agents aware of your concerns and document your observations and objections.
- ✓ **Determine whether employees are being detained.** People in the area to be searched can be temporarily detained, and others outside the search area may be barred from entering it, to allow the search to proceed expeditiously and without interference. However, employees are not required to give interviews, and individuals who are not identified in the warrant itself may not be searched except when the agents have at least an “articulable and individualized” suspicion of wrongdoing on their part. Nonetheless, under the pretense of securing the premises, agents may attempt to confine personnel to certain areas, limit use of telephones, and pat down individuals and search their personal belongings. Asking agents whether individuals are under arrest will usually deter them from unreasonably restricting movement or telephone use.
- ✓ **Advise employees of their rights.** Agents often attempt to question employees, so it is important that all employees understand their rights. It is generally permissible to advise employees that:
 1. They may, but are not required to, answer agents’ questions and whether to do so is entirely up to them.
 2. If they do choose to speak to agents they:
 - a. must tell the truth and could be subject to criminal prosecution for any false statements.
 - b. can set conditions, such as having counsel present for any questioning.
 3. They should ask to speak with counsel if questions veer into potentially privileged communications. Be careful not to give advice to employees that could be construed as an instruction not to cooperate with the agents and do not suggest or imply that a decision to speak with agents will be viewed unfavorably by the company. Such actions can lead to obstruction charges. It is best to provide this advice in writing to avoid subsequent disputes regarding what employees were advised to do. A sample Search Warrant Notice to Employees is included in this handbook.

- ✓ **Consider sending employees home.** Because the search is likely to disrupt work, it may be best to send non-essential personnel in affected areas of the facility home for the day.
- ✓ **Object to any review or seizure of privileged data, including legal communications.** If the agents insist on seizing legally privileged documents despite your objections, immediately contact the responsible prosecutor. If the seizure goes forward, propose that you gather the documents under the agents' supervision and seal them so that they cannot be opened without breaking the seal. This can defer government review of privileged documents until the privilege issue is resolved.
- ✓ **Make a record of events as they unfold.** Keep detailed notes during the search (to the extent possible) to support a possible challenge to the legality of the search and to memorialize information concerning the scope and nature of the investigation. Depending on the number of agents involved, additional attorneys or paralegals may be required to properly monitor all the agents' activities.
- ✓ **Ask to be present when the agents inventory the property to be seized.**
You are entitled to a receipt of the property before the agents leave. Typically, the agents will provide you with a copy of their inventory.
- ✓ **Make your own inventory of the seized property, including photographs, if possible.**
Agents' inventories can often be sparse and difficult to rely on when identifying what was seized.
- ✓ **Ask for copies of seized electronic media.** Computer searches are generally executed either by making electronic copies of files on-site or by simply seizing the computers and reviewing their contents off-site. Typically, the search warrant itself will address the procedures the agents are required to follow. The agents may not be required to provide you with electronic copies of seized computer files but may do so if you ask. If necessary, arrangements can usually be made to obtain electronic copies after the search to minimize the adverse impact on the company's operations.
- ✓ **Ask for split samples.** When agents seize samples, such as in environmental investigations, ask for a split sample (i.e., a portion of the same sample being seized). If a split sample is refused, take your own parallel sample (ideally under monitored circumstances after the agents depart).
- ✓ **Advise the lead agent of any classified documents that are on the premises and/or seized.** Classified documents are not exempt from search and seizure, but the agents should be advised of the status of such documents if the company has an obligation to protect classified information. If classified documents are seized, notify the agency with jurisdiction over the information immediately. Similarly, notify the agents if they confiscate any proprietary or trade secret information.
- ✓ **Advise employees not to discuss the search with others, except legal counsel.** Direct all communications regarding the status of the search to legal counsel to avoid internal chatter (and especially external publicity). However, do not instruct employees not to speak with agents.

NOT This

- ✗ **Do not attempt to prevent the search from taking place or obstruct the agents executing the warrant. Instruct employees likewise.** Such actions can result in criminal sanctions. In addition, agents executing a search warrant are authorized to use force.
- ✗ **Do not remove or destroy documents to prevent their seizure.** Remind employees that removing, concealing, altering, destroying, or deleting documents to prevent their seizure is strictly prohibited and could lead to criminal prosecution.
- ✗ **Do not consent or otherwise give your permission to search any area or to seize any property.** Be very clear that you will not consent to a warrantless search or a search that exceeds the warrant's scope, at least until you have an opportunity to consult with outside counsel. Questions may arise concerning the warrant's coverage, or the agents may believe that a broader search is necessary. For example, the agents may seek to search or seize an item not identified in the warrant itself, such as a laptop computer. In these situations, the agents may seek consent to search beyond what is authorized in the warrant. Do not give it.
- ✗ **Do not volunteer substantive information.** A search warrant does not require you or any other employee to provide directions or guidance to the agents. You are not required to show them the location of documents or other property, or otherwise assist in the search. However, you may provide some assistance as a simple courtesy when the answer is obvious or to prevent unnecessary disruption by the agents in locating their objective.
- ✗ **Do not tell employees not to speak with agents.** You can and should advise employees of their rights, but do not instruct them not to speak with the agents or even imply that speaking will have unfavorable consequences.

Government Subpoenas/Inquiries

Preservation

A document subpoena, preservation notice, or other similar investigative demand can raise a host of thorny issues, particularly for large companies that may possess huge amounts of material, including electronically stored information (ESI). If the government also subpoenas a company employee or document custodian for testimony, consult outside counsel regarding the appropriate responses and options.

Companies under subpoena for documents have an affirmative duty to identify, locate, and preserve all relevant information and to produce all non-privileged responsive documents, including ESI.



For any government subpoena or inquiry, the initial focus should be on preservation efforts, which are critical. Preservation can impact both the ability to conduct an effective internal investigation and the ability to respond to the government's requests.



Failure to preserve is a frequent misstep in the initial stages of an investigation. This section provides guidance to help execute appropriate preservation requirements and avoid the common missteps.

Preservation Checklist

DO This

- ✓ Involve qualified outside white-collar counsel as soon as possible.
- ✓ Understand the duty to preserve, including electronic records that are documents (e.g., texts, chats, recordings, etc.).
- ✓ Quickly distribute a [Preservation Notice](#) to employees who may possess the documents listed in the subpoena or that are otherwise relevant.
- ✓ Implement back-end IT holds on relevant data systems and employee accounts.
- ✓ Suspend any scheduled document destruction or deletion protocols.

NOT This

- ✗ Do not allow employees to destroy, hide, or manipulate any data.
- ✗ Do not immediately start rummaging through files and physically removing documents described in the subpoena.

Detailed Guidance

DO This

- ✓ **Involve outside counsel as soon as possible.** Quickly consult and coordinate with qualified outside white-collar counsel in connection with the investigation that gave rise to the subpoena or document preservation notice. It is often possible to negotiate with prosecutors and investigating agencies to narrow the scope of a subpoena and adjust the timing of the response. Start those negotiations promptly.
- ✓ **Understand the duty to preserve.** The duty to preserve may arise even before the arrival of a subpoena or other process. The duty arises whenever a government investigation is threatened, pending, or can be reasonably anticipated. A government investigation need not have commenced and a subpoena need not have been issued for the duty to preserve to arise, and violations can have significant consequences, potentially including obstruction charges under 18 U.S.C. § 1519 (“Whoever knowingly alters, destroys... [or] falsifies... any... document... with the intent to impede, obstruct, or influence the investigation... of any matter within the jurisdiction of any department or agency of the United States... or in relation to or contemplation of any such matter or case, shall be fined... [or] imprisoned not more than 20 years, or both”).
- ✓ **Quickly distribute a Preservation Notice.** Once the duty to preserve arises, company counsel must move quickly to distribute a Preservation Notice that tracks the government’s information request (if available) and ensures that employees are on notice of the categories of information that must be preserved. Draft and issue the Preservation Notice as soon as possible. The potential consequences flowing from a post-duty loss or destruction of potential evidentiary material are too serious to delay issuing the Preservation Notice. The parameters of a Preservation Notice can always be expanded or modified as you learn more. A sample Preservation Notice is included in this handbook.
- ✓ **Promptly notify employees who may possess the documents listed in the subpoena.** Detail what is to be produced; do not circulate copies of the subpoena itself. To the extent the subpoena calls for ESI, such as computer files and emails, promptly notify your IT personnel and involve them in the compliance efforts.
- ✓ **Suspend any scheduled document destruction or deletion protocols.** Assess whether any relevant document repositories are scheduled for routine destruction, and if so, suspend the destruction pending resolution of the matter. Similarly, turn off any auto-delete protocols that impact relevant data systems or employees.



NOT This

- ✗ **Do not allow employees to destroy, hide, or manipulate documents.** In addition to issuing a Preservation Notice to relevant employees, make sure to implement back-end IT holds on relevant data systems and employee accounts. This prevents employees from personally deleting relevant documents stored on the company's network.
- ✗ **Do not start rummaging through files and physically removing documents described in the subpoena.** The scope of a subpoena's document requests may be narrowed in negotiations, so hold off on gathering documents until the scope is final. At that point, collect documents for production in a systematic way, keeping a record of sources and locations, and avoid situations where responsive documents could be misplaced.

Other Crises

Companies may encounter crisis situations beyond searches and subpoenas. Below are examples of other common crises and specific strategic considerations for each.

“We’ve Got a Whistleblower.”

A whistleblower is a person (often an insider) who raises an allegation of wrongdoing within the company. Whistleblowers may make their allegations internally (for example, to other people within the company) or externally (to government agencies, the media, or both). Certain federal and state statutes enable whistleblowers to initiate lawsuits targeting allegedly unlawful or fraudulent business practices and protect them from retaliation. These statutes offer the lure of huge monetary rewards for the whistleblower.

Do not retaliate: Unless otherwise required by government contract or regulation, resist the urge to immediately confront the suspected whistleblower, and do not summarily impose disciplinary action, such as suspension or termination. Instead, contact qualified counsel immediately.

“We Had a Ransomware Attack.”

Any organization that possesses data is at risk for a cybersecurity incident (i.e., a hack) where a malicious actor gains access to internal computer or data systems and either takes company data or prevents access to it. Every organization needs to have a written plan for what it is going to do in the event of a cyber incident or data breach. It is a good idea to run a [tabletop or training exercise](#) at least annually to test the incident response plan and iron out any issues outside the pressure-cooker environment of an actual cyber incident. The “who,” “what,” and “when” of notifying others outside the company about the cyber incident is a sensitive area fraught with potential risk to the company and should be handled with care. Some cyber incidents can be handled in-house. But factors such as the sensitivity of any data exfiltrated by the bad actors, the need to report a material incident within a certain time period or other regulatory requirements, and the likelihood that litigation will ensue, may warrant engaging outside counsel to assist with incident response under the umbrella of attorney-client privilege.

“Law Enforcement is Informally Reaching Out.”

The initial contact from law enforcement can be a visit or phone call by an agent or officer who has no search warrant or subpoena but wishes to talk to the company’s employees. Although cooperation with law enforcement can sometimes yield benefits, companies should proceed with caution. Attempt to determine the subject of the inquiry and then politely delay the interviews so you can contact qualified outside counsel immediately. Outside counsel can contact the agent and advise you on how best to proceed. Counsel may determine that the interviews should not proceed without the presence of an attorney or should not take place at all.



“An Employee is Seriously Injured.”

While fatal and nonfatal injuries to employees are tragic, workplace accidents can also pose serious legal challenges. These include not only personal injury suits but also inquiries from state and federal regulators such as OSHA. Further, an accident involving serious injury or death may attract press attention and/or a criminal investigation. If regulatory agents such as OSHA investigators arrive to investigate the incident, immediately contact qualified counsel. In the meantime, do not attempt to impede or otherwise interfere with the agents or inspectors. If they wish to interview employees, respond as you would in the context of such requests during a search or informal contact, as discussed above.

“There’s a Reporter on the Phone.”

A reporter’s telephone call or visit is often the first sign of a burgeoning problem. Instruct employees to refer press inquiries to either the appropriate public affairs professional or in-house counsel. If a press inquiry is expected due to a public incident, whether a company-related accident or some type of law enforcement activity, reiterate and re-emphasize the policy of passing press inquiries on to the appropriate company representative. Initial responses to media inquiries should be brief, non-specific, and provided in writing; do not engage in a free-ranging conversation with reporters prior to learning all the facts. Involve qualified outside counsel before responding to any media inquiry.

“An Employee is Accused of Personal Misconduct/Harassment.”

Significant legal fallout and reputational damage occurs when a company mishandles allegations of personal misconduct and harassment by one of its employees. To ensure that these claims are handled properly, companies should make sure that they provide proactive training, review and update harassment and misconduct policies, and immediately elevate complaints to the in-house or outside counsel for assessment and action. Establish clear reporting requirements for supervisors and staff to ensure that allegations are properly elevated.

Samples

Notices related to investigations should follow a clear format. You can use the following examples to notify employees of a government search warrant (including interview rights), their preservation obligations, and the conditions under which counsel is interviewing them on behalf of a company (Upjohn advisory). These samples are generic and are a guide for creating a more tailored document. We always recommend that companies enlist experienced white-collar counsel when confronting a crisis.

Digital Versions



**Search Warrant
Notice to Employees**



Preservation Notice



**Upjohn
Advisory**

Search Warrant Notice to Employees

CONFIDENTIAL

To: All Employees

From: [Legal Counsel]

Date: [Date]

As you may know, government agents have executed a search warrant on the company's premises, and apparently are conducting an ongoing investigation that involves the company. The company intends to cooperate in that investigation. However, since these are complicated matters involving important legal issues, we are distributing this notice to provide you with specific guidance regarding this situation.

1. Preserve documents—It is important that no one remove, hide, alter, or destroy any relevant documents, papers, computer files, etc., while this investigation is pending. If you are unsure whether something is relevant, preserve it. We do not want any innocent or routine destruction of documents to be misinterpreted. We are distributing a separate notice with specific instructions regarding document preservation. If you have any questions, please contact [legal counsel] at [email or phone number].
2. Requests for additional information or documents—If you receive any requests from government agents, news media, or other third parties for additional information or documents, you should refer the requestor and report the request immediately to [legal counsel], who will handle such matters.
3. Maintain confidentiality—We are working with legal counsel to understand and handle this situation. However, at this moment, we ask that you please not discuss today's events with anyone, including your fellow employees, given that it is an ongoing investigation. However, if you have any questions or concerns, you can always reach out to [legal counsel].
4. Remote / offsite employees—If you are working remotely today or are otherwise not in the office, please plan not to come into the office until further notice.
5. Requests for interviews—Government agents may attempt to contact you at your office or home and request to interview you. You are free to talk to them, but you are not required to submit to an interview. You have the right to confer with an attorney first and to insist on scheduling any interview at a time and place that is convenient. An attorney can meet with you in advance and advise you. Also, by being present at any interview, an attorney can try to avoid any confusion you may have regarding the government agents' questions. The company will arrange for an attorney to talk to you if that becomes necessary and you so desire. If you speak to the government, you must always tell the truth. If you are contacted by government agents, please let [legal counsel] know.

We know these matters are a distraction and regret any concern this may cause. We appreciate your patience and cooperation.

Preservation Notice

To: [Distribution list, stated here or attached]

From: [GC or other senior in-house lawyer; if company has no in-house counsel, the notice may be issued by a senior executive uninvolved in the matter under investigation, or, as a last resort, by outside counsel]

Date: [Date]

Confidential Document Preservation Notice

This document preservation notice is strictly confidential and should not be discussed inside or outside the company other than questions directed to [designated contact person's name] to ensure compliance. [NOTE: Consider assigning multiple contacts, if warranted in light of the size of the distribution list and anticipated burden of responding to related questions.]

[For a purely internal investigation:]

An internal inquiry is being conducted by company counsel regarding [general description of subject matter of investigation]. The fact that such an inquiry is being conducted [is not cause for alarm, but it] should of course be **treated as confidential** within the company.

In order to facilitate the internal inquiry and comply with the company's legal obligations, **it is vital that all documents and data described below are preserved** and that all routine or other disposal, destruction, or deletion of such materials be suspended until further notice.


[In response to a government subpoena:]

[Company] has received a subpoena from [government office or agency] that will require the collection and production of certain company documents in connection with an investigation of [general description of subject matter of investigation]. [Company] intends to cooperate with the [office/agency] investigation and will fully comply with the subpoena. The fact that such an inquiry is being conducted [is not cause for alarm, but it] should of course be treated as confidential within the company.

In order to comply with the subpoena, it is vital that all documents described below are preserved, and that all routine or other disposal, destruction, or deletion of such materials be suspended until further notice.

Types of Documents: Specifically, you must take all necessary steps to ensure that the following types of documents are preserved:

- [specify categories of documents to be preserved; if responding to a subpoena, adhere to the specifications in the subpoena and edit sparingly—use an attachment if necessary]



What Are Documents and Where Are They Located: The term “documents” include all types of hard-copy and electronic documents and data, regardless of whether located on or at **company or personal** premises, devices, or accounts. **If you are uncertain** as to whether something is a document that should be preserved, **err on the side of preservation**. The documents identified above must be maintained regardless of where they are located or the form in which they are stored, for example:

- Hard-copy documents
 - in your office
 - in common or shared storage areas
 - at any company facility
 - in off-site storage facilities
 - at your home
 - at any other location
- Electronic documents and data, **including text messages and chat conversations, regardless of the platform or application**
 - on computer servers
 - in databases
 - on desktop or laptop computers
 - in email accounts
 - in instant-messaging accounts
 - in voicemail boxes
 - on smart phones or other devices
 - in cloud storage repositories
 - on portable electronic media such as external hard drives, thumb drives or CDs

There is no distinction between “official” company files and your “personal” files. All potentially relevant documents that you wrote, compiled, or received must be preserved, including any copies you have saved separately from any “official” or “company” file. This is so even if such documents are maintained on your personal platforms, cloud storage, social media accounts, personal communications services and applications, personal devices, or other repositories that you control.

Other Instructions

- These document preservation instructions take precedence over all other document-management policies or programs. Please take all necessary steps to suspend routine document destruction activities that might threaten covered documents, including documents that may be stored off-site (e.g., on your phone or in the cloud), and the automatic deletion or overwriting of data. This includes changing or updating settings on your phone or other devices to turn off auto-delete functions or expiration periods on applications, that may contain documents or data subject to this notice to ensure such documents are preserved.
- **Again, if you are in doubt** as to whether any documents should be preserved, you should err on the side of preservation.
- Originals **and** all copies, including drafts, of relevant documents must be preserved.
- [remove when distribution list is not shared (e.g., when even the identity of those involved is sensitive)]
If you are aware of anyone who has custody of or access to the categories of documents described above and was not included on the distribution list for this notice, please notify [designated contact person's name] immediately.
- Do not forward or distribute this notice.

Your compliance with the instructions in this notice is essential. Any alteration, removal, or destruction of relevant documents or data may be a violation of law that could result in adverse consequences for the responsible individual(s) and/or the company.

Please promptly confirm by reply email to [designated contact person's name and email address] that you have received, reviewed, and will comply with the instructions in this notice.

Please also keep in mind the confidential nature of this preservation notice and the related inquiry.

If you have any questions about these instructions, please call [designated contact person's name] at [phone number].

Thank you for your cooperation.

Upjohn Advisory

I am a lawyer for or from the Company. I represent only the Company, and I do not represent you or any other employee personally.

I am conducting this interview to gather facts in order to provide legal advice to the Company. This interview is part of an investigation to determine the facts and circumstances of X in order to provide legal advice to the Company about how best to proceed.

Your communications with me are protected by the attorney-client privilege. But the attorney-client privilege belongs solely to the Company, not you. The Company alone may decide to assert or waive the privilege [and disclose this discussion to third parties such as federal or state agencies, at its sole discretion, and without notifying you].

In order for this discussion to remain subject to the privilege, it must be kept in confidence. In other words, with the exception of your own attorney, you may not discuss the questions you were asked or how you responded.

Do you have any questions? Are you willing to proceed?

In-House CLE Offerings

Crowell & Moring routinely provides CLE presentations to corporate legal departments and business teams. Some of our most popular topics are below. Please [contact us](#) if you would like to schedule a training or discuss a customized offering to meet your specific needs.

Nuts and Bolts: Conducting an Internal Investigation

Internal investigations have become an important exercise in good corporate governance and can be initiated for a variety of reasons. This program focuses on what in-house counsel need to consider when running an internal investigation. Topics include:

- Scoping the investigation so that it is appropriate and not overly broad or too narrow.
- Issuing preservation notices/holds.
- Developing a plan for an internal review that will withstand the scrutiny of internal and external stakeholders, as well as regulators.
- Addressing differences in attorney-client privilege when the review is multinational.
- Conducting employee interviews and using Upjohn advisories.
- Determining whether an investigation report is appropriate.
- Addressing whistleblowers (and avoiding retaliation claims).

Attorney-Client Privilege: Fundamentals and Best Practices

The program addresses how to preserve the attorney-client privilege during internal investigations. It examines the elements of privilege law and best practices for preserving it during internal investigations.

Protections and Pitfalls Concerning Cross-Border Privilege Claims

Business operations, government investigations, and litigation are increasingly global. One matter may involve many different countries. Each jurisdiction has its own rules on legal privileges and protections, and its own views on how they relate to in-house counsel, outside counsel, and third parties. This CLE provides an overview of these rules in key jurisdictions, how the rules interact when the work crosses borders, along with practical tips and best practices for preserving privilege and avoiding pitfalls.

Visit Us Online

To learn more about Crowell’s investigations team, or to download electronic versions of some of the documents in this guide—including a PDF of the handbook—visit our [website](#).

Disclaimer

The content and samples in this handbook are intended to serve as general guidance. Qualified legal counsel should always be consulted when facing an investigation.



Crowell & Moring is an international law firm with operations in the United States, Europe, MENA, and Asia. Drawing on significant government, business, industry, and legal experience, the firm helps clients capitalize on opportunities and provides creative solutions to complex regulatory and policy, litigation, transactional, and intellectual property issues. The firm is consistently recognized for its commitment to pro bono service, as well as its comprehensive programs and initiatives to advance the professional and personal development of all members of the Crowell community.

Attorney advertising. The contents of this briefing are not intended to serve as legal advice related to any individual situation. This material is made available by Crowell & Moring LLP for information purposes only.

crowell.com