Crowell

Corporate Crisis Handbook

A Desktop Investigations Guide For In-House Counsel

About Crowell & Moring

For nearly forty years, Crowell & Moring has successfully defended clients worldwide in criminal and regulatory investigations, trials, and enforcement actions. Our practice spans investigations – grand juries, federal agencies, federal inspectors general, Congress, state attorneys general, and a range of other investigative entities. Our clients include multinational corporations, closely held businesses, boards of directors, partnerships, members of executive management and other individual clients. Our team has successfully dealt with innumerable "crisis" situations such as those described in this Handbook, as well as the investigations that may flow from them.

Bringing together a battle-tested team of litigators, former prosecutors, and regulatory attorneys to craft strategies that succeed and bring clients peace of mind.

Named to the *Global Investigations Review*'s "GIR 100," our lawyers have represented clients in matters spanning more than 80 countries and six continents around the globe.

Crowell & Moring has a wide-reaching international practice, including highly experienced white collar and regulatory attorneys in the firm's Washington, New York, California, and European offices. We have the rare blend of insight, experience, maturity and judgment that can only be gleaned from a team that includes lifelong defense lawyers, former prosecutors, enforcement attorneys, and agency officials, many of whom served at high levels within the U.S. Department of Justice, U.S. Attorney's offices, the Securities and Exchange Commission, the FBI, OFAC, FinCEN, and DHS. We also have some of the most widely respected practitioners in the subject matter areas that are often the focus of such investigations, including AML, antitrust, cybersecurity, trade, FCPA, financial fraud, tax, health care, public corruption, insider trading and trade secrets, among others. We carefully structure each engagement team to provide our clients with the benefits of this collective experience and expertise.

Learn more about Crowell & Moring at crowell.com.

Table of Contents

You start getting panicked phone calls and emails from top management, seeking your guidance. Something must be done quickly.

The following guide is intended to assist those who find themselves in such an unhappy situation. It will provide guidance about what to do and, of equal importance, what not to do, in the early minutes and hours of the crisis.

When Crisis Strikes

Crisis can hit in many forms, including:

Law enforcement agents with a search warrant burst into your company's offices and begin searching all of your files, copying your computers and electronic devices, and speaking to your employees.

Two FBI agents arrive at your business and ask to speak to particular employees (or they show up at the employees' homes).

A news reporter calls with questions about certain payments in a foreign country made by a company sales representative to a government official.

A current employee becomes a "whistleblower" and provides confidential information and documents to government agents.

Your chief information security officer informs you that your business network has been attacked by ransomware, all of your systems are inaccessible, and there is a demand that you pay a $5 million ransom to restore your systems.

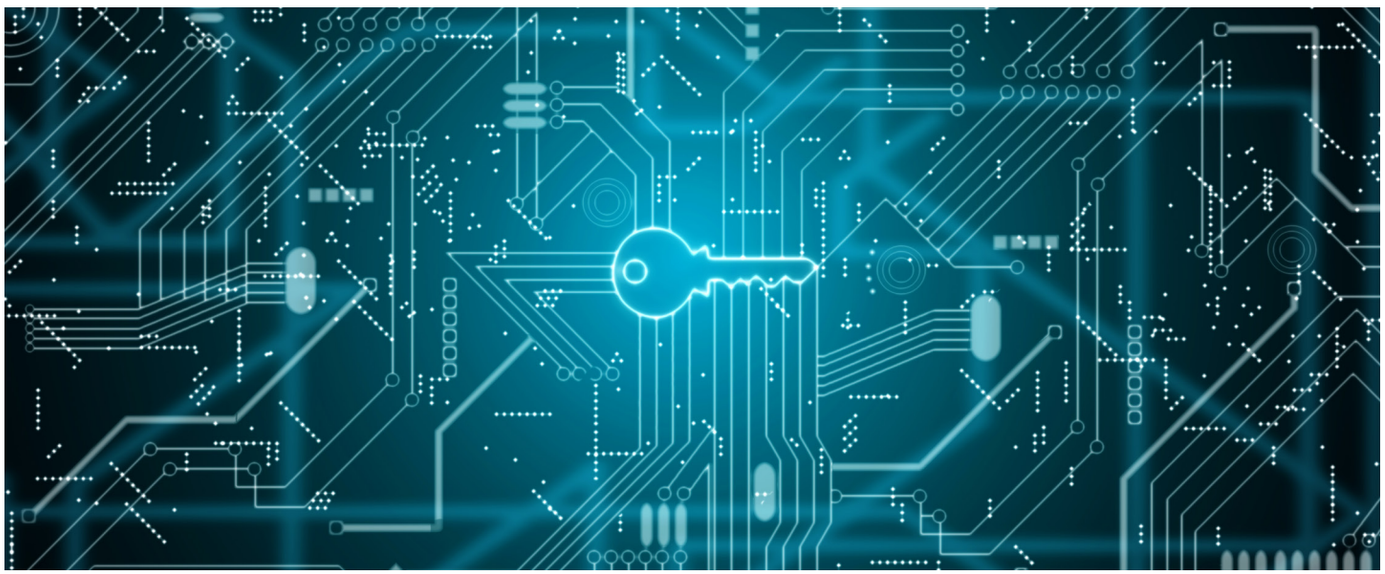
A process server or federal agent shows up with a grand jury (or similar) subpoena for documents or testimony, or both.

Your VP of Investor Relations gets a telephone call from the SEC's Enforcement Division. Simultaneously, a "Document Preservation" notice from the SEC arrives in your inbox.

An employee is seriously injured or killed in a work-related accident.

Your employee is stopped and his electronics are searched at U.S. customs after returning from international travel and she is carrying sensitive corporate documents or trade secrets.

The head of HR informs you that one of the company's executives has been accused of sexual harassment or misconduct.



Crisis scenarios often necessitate the launch of an internal investigation to determine the company's legal exposure. Understanding the phases and components common to investigations is key to avoiding unnecessary missteps.

Investigations

Common Goals of an Investigation

- Understand the facts
- Understand the cause
- Maintain privilege
- Assess exposure to criminal, regulatory, civil liability
- Implement corrective actions (remediation/mitigation)
- Minimize disruption to the business
- Determine disclosure obligations
- Avoid criminal referral/prosecution/ and civil enforcement action
- Avoid damage to parallel private civil litigation

Conducting an Investigation – Maintaining the Privilege

Facts are not privileged, but legal analysis and conclusions drawn from facts are privileged. Confidential communications between employees and counsel for the company for the purpose assessing legal issues or providing legal advice to the company are protected by the attorney client communications privilege. Likewise, the work product of investigations conducted by or at the direction of counsel for the purpose of providing legal advice to the company (in anticipation of litigation, broadly defined) is generally privileged. The privilege belongs to the company, not to any individual officer or employee. Accordingly, to maintain privilege over the investigative work product, always:

- Document that the investigation's purpose is to provide legal advice to the company

- Have counsel conduct the investigation or, at a minimum, actively direct non-attorneys conducting the investigation under written instruction from counsel

- Take extra precautions in non-U.S. jurisdictions
  - The attorney client privilege does not always extend to in-house counsel

  - Not all jurisdictions recognize, or apply as broadly, attorney-client communications privilege or the work product doctrine

Employee Interviews– Preserving the Privilege

To preserve and protect the company's privilege over the investigation, it is critical that counsel make clear to interviewed employees that no attorney-client relationship exists between counsel and the employee. Always provide an *Upjohn* warning.

- *Upjohn warning*: at the outset of the interview, advise the employee that counsel represents the company, not the employee, that the purpose of the interview is to gather information to provide legal advice to the company, that the interview itself is confidential and privileged (not the facts), that the company alone can decide to waive the privilege and disclose the discussion to third parties, including the government; that the employee should not discuss the substance of the interview with others but can discuss the underlying facts (e.g., with a regulator).

- *Memorialize the interview*: a written record of the interview should be prepared and preserved. It should include that an Upjohn warning was provided and acknowledged by employee and that the interview memo is not a transcription and contains counsel's mental impressions.

Be Prepared for a Search

No company expects to be the subject of an unannounced search by armed federal agents. Nonetheless, it is best to prepare for the worst. Advisable steps include:

- Clearly mark privileged documents and maintain them separately from non-privileged material;
- Maintain copies of essential business records (including records stored on personal computers) off premises;
- Ensure that at least one lawyer at each company facility has been trained regarding the proper response to a search warrant. Management at facilities where there is no lawyer should know whom to call in the event of a search;
- Identify outside counsel experienced in criminal law before the need arises, and have counsel's contact information readily available and distributed to key personnel; and
- Develop a plan for closing the facility in case of such a search.

The Search Warrant Checklist

See detailed guidance for search warrants on page 10.

DO This

- Identify and meet with the lead agent. Learn the identity of the supervising prosecutor.
- Ask for a copy of the warrant and review it carefully.
- Determine whether agents are detaining employees.
- Advise employees of their rights – including the right to counsel. (See attached sample "Notice to Employees.")
- Consider sending employees home. Object to the seizure of privileged documents.
- Make a record of events as they unfold. Ask to be present when agents make an inventory of seized materials.
- Make your own inventory of seized materials.
- Ask for copies of seized computer files.
- Ask for split samples.
- Advise the lead agent of any classified documents that are seized.

NOT This

- Do not interfere with the search.
- Do not allow anyone to alter, hide or destroy documents.
- Do not consent to the search of any area or seizure of any materials.
- Do not volunteer substantive information.
- Do not instruct or encourage anyone not to speak with the agents.

The Government Subpoena/Civil Investigation Demand Checklist

See detailed guidance for subpoenas on page 12.

DO This

- Issue a preliminary document "Hold Order" to all relevant personnel that prohibits the destruction, "loss" or alteration of any documents that arguably fall within the scope of the subpoena. (See attached sample "Preservation Memo/Hold Order.")
- Promptly notify officers and employees who may possess the documents listed in the subpoena and detail what is to be produced; do not circulate copies of the subpoena itself.
- To the extent the subpoena calls for electronically stored information, 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. Turn off any "auto-delete" programs.
- For an SEC or CFTC subpoena, obtain a copy of the Formal Order of Investigation.

NOT This

- Do not allow employees to destroy, hide, or manipulate documents.
- Do not immediately start rummaging through files and physically removing documents described in the subpoena. Instead, wait until qualified counsel and their paralegals, and perhaps document collection and reproduction experts, get involved.

The Cybersecurity and Privacy Incident Checklist

See detailed guidance for responding to a cyber incident on page 13.

DO This

- Promptly contact your pre-identified cybersecurity/privacy law firm and a forensic vendor.
- Begin executing your incident response plan for cybersecurity or privacy incidents, and identify a team lead.
- Establish an attorney-directed investigation and communication channel to maximize privilege in connection with the incident response.
- Identify and preserve evidence including computer logs, sensitive business information, communications, and other important network activity.
- With forensic professionals identify and isolate the vulnerability or attack and carefully document your steps.
- Take necessary and appropriate security actions such as password resets, carefully documenting such steps and in coordination with your professional forensic vendor.
- Attorneys should conduct any appropriate interviews of employees.
- Provide instructions and guidance to employees as necessary and appropriate.
- Analyze the business impact and potential data loss.
- Evaluate whether law enforcement should be engaged.
- Analyze your legal reporting obligations under various federal and state laws, and your contractual obligations.

NOT This

- Do not continue as business as usual.
- Do not connect additional devices to potentially infected systems.
- Do not disconnect or shut down computers hoping the problem will go way.
- Do not perform self-help to try to remediate the problem without professional forensic vendors.
- Do not share non-public information about a breach, nor should you decide to dump all your company stock if you are in possession of material non-public information.
- Do not communicate with ransomware attackers without evaluating the risks and potential benefits with legal and forensic professionals.

Guidance For Other Potential Crisis

A. "Informal" Visits by Law Enforcement Agents

Sometimes, the initial contact with law enforcement is a visit or phone call by an agent or officer who has no search warrant or subpoena, but wishes to talk to you or your company's employees. Although cooperation with law enforcement can often yield benefits, companies nevertheless should proceed with caution. You should attempt to determine the subject of the inquiry and then politely delay the interview(s), so that you may contact qualified outside counsel immediately. Outside counsel can make contact with the agent, and advise you on how best to proceed. It may be determined that any such interviews should not proceed without the presence of an attorney, or should not take place at all.

B. "There's a Reporter on the Phone"

Sometimes, a telephone call or visit from a reporter is the first sign of a burgeoning problem. Employees should be instructed 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, the company should reiterate and re-emphasize the policy of passing press inquiries on to the appropriate company representative. Generally, any initial response to media inquiries should be brief, non-specific, and provided in writing; it is not wise to engage in a free-ranging conversation with reporters prior to learning all the facts. If possible, you should involve qualified outside counsel immediately, prior to responding to any media inquiry.

C. "An Employee has been Seriously Injured" (or Worse)

In addition to the tragedy of injuries to or the death of an employee, a serious accident can also present serious legal challenges to a company on whose premises the accident occurs. These include not only personal injury suits but also inquiries from state and federal regulators, such as OSHA. Further, an accident causing serious injury or death may attract press attention. If regulatory agents, such as OSHA investigators, arrive to investigate the incident, you should immediately contact qualified counsel. In the meantime, you should not attempt to impede or otherwise interfere with the agents or inspectors. If they wish to interview employees, you should generally respond as you would in the context of such requests during a search or informal contact, as discussed above. It is often critical that any such interviews be conducted in the presence of qualified counsel, if at all.

D. "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. These statutes offer the lure of huge monetary rewards for the whistleblower, and some reward whistleblowers just for reporting information, without filing a lawsuit. While once largely limited to instances of fraud by government contractors, these statutory schemes are now being more broadly applied to other scenarios, including alleged securities fraud and bribery of foreign officials.

Perhaps the most important initial consideration, upon learning of the existence of a possible employee-whistleblower, is to avoid taking any swift action that may appear retaliatory. 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.

E. Report of Sexual Misconduct or Harassment

Significant legal fallout and reputational damage occurs when a company mishandles allegations of sexual misconduct and harassment by one of its executives. Increasingly, any allegation of sexual misconduct or harassment – recent or from years past – leads to serious ramifications for a corporation, regardless of the seniority of the accused. Claims of sexual harassment and misconduct can longer be confined to the purview of the human resources department. Proactive training, review and updating of policies and immediate elevation of complaints to the in-house attorneys for assessment and action is critical. Establishing clear reporting requirements for supervisors and staff is key to ensure that allegations are properly elevated. Following receipt of an allegation, counsel must respond as they do with any threat of litigation with immediate preservation of evidence and issuance of the appropriate document hold notices. Counsel should consider whether in-house counsel should conduct the investigation into the allegations, or if outside counsel for the company may do so. In certain circumstances, it may be appropriate for the outside counsel conducting the investigation to report to the Board or subset of independent directors. Alternatively, management or the Board may direct outside counsel to conduct an entirely independent investigation, but the latter investigation provides no privilege protection for the company.

Detailed Guidance on Responding to a Search Warrant

Immediately contact outside counsel with white-collar expertise.

Do not attempt to prevent the search from taking place or obstruct the agents executing the warrant. Employees should be instructed likewise. Such actions can result in criminal sanctions. In addition, agents executing a search warrant are authorized to use force.

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.[1] Ask the lead agent for information concerning the status of the company (e.g., target or subject of the investigation, or neither) and the nature of the allegations being investigated. Also ask whether any employees have been or are being interviewed, and, if so, request that legal counsel be present at any such interviews.[2] Do not engage in a dialog or debate with the agents regarding the factual basis of the investigation.[3]

Obtain and review the search warrant. The agents are required to provide a copy of the warrant. Request a copy. Review the warrant as soon as possible to gauge whether the search is 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 agents are detaining employees. Persons 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. Individuals who are not identified in the warrant itself may not be searched except where the agents have at least an "articulable and individualized" suspicion of wrongdoing on their part. However, under the pretense of securing the premises, agents may attempt to confine personnel to certain areas, to limit use of telephones, and to pat down individuals and search their personal effects. Asking agents whether individuals are under arrest will usually prompt them to desist from unreasonably restricting movement or telephone use.

Advise employees of their rights. It is common for agents to attempt to question employees, including meeting with them individually in an office on the searched premises. It is important, therefore, that all employees understand their rights. Be very careful not to give advice to employees that could be construed as an instruction not to cooperate with the agents. Such actions can lead to charges of criminal obstruction. It is generally permissible, however, 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, and (b) can set conditions, such as having company counsel present for any questioning. You should not suggest that a decision to speak with agents will be viewed unfavorably by the company. It is best to provide such advice in writing in order to avoid subsequent disputes regarding what employees were advised to do. A sample of such a "Search Warrant Notice to Employees" is included at the end of this handbook. It can also be found at http://www.crowell.com/PDF/Sample-Notice-to-Employees.pdf

Do not remove or destroy documents to prevent their seizure. Remind employees that removing, concealing, altering, destroying or deleting documents is strictly prohibited and could lead to criminal prosecution.

Consider sending employees home. Because the search is likely to substantially disrupt work, it may be best to send non-essential personnel in affected areas of the facility home for the day. This will also reduce the likelihood that agents will attempt to interview employees before the employees are advised of their rights and options.

Do not consent or otherwise give your permission to search any area or to seize any property. In the event

1 Government attorneys typically do not accompany the agents to the search. However, they will often be available by telephone.

2 Keep in mind that search warrants typically do not authorize agents to conduct interviews on the company's premises. You and your employees are not required to consent to such interviews or to permit company property to be used for law enforcement purposes.

3 If in-house counsel is concerned that he or she is or may become a target of the investigation, counsel should avoid substantive discussion with the agents or prosecutor regarding the apparent subject matter of the investigation. It is best if outside counsel or conflict-free, in-house counsel take the lead in representing the company's interests in those hopefully rare situations.

of any question concerning the warrant's coverage, or if the agents believe that a broader search is necessary or that an item not identified in the warrant itself, such as a laptop computer, should be searched, they may seek consent to search beyond what is authorized in the warrant. Do not give it. Be very clear that you will not consent to a warrantless search, at least until you have an opportunity to consult with outside counsel.

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, some assistance can be provided as a simple courtesy when the answer is obvious or to prevent unnecessary disruption by the agents in locating their objective.

Object to any review or seizure of privileged documents, including legal communications. If the agents insist on seizing legally privileged documents despite your objections, immediately contact the responsible Assistant United States Attorney. 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.[4] You can thus prevent 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 generally to collect information concerning the scope and nature of the investigation. Depending on the number of agents involved, additional attorneys and/or paralegals may be required to properly monitor all of the agents' activities.

Ask to be present when the agents make an inventory of the property to be seized. You are entitled to a receipt for the property before the agents leave. Typically, the agents will provide you with a copy of their inventory as the "receipt."

Make your own inventory of the seized property, including photographs if possible. Agents' "inventories" often can be sparse and unhelpful.

Ask for copies of seized electronic media. Computer searches are generally executed either by making electronic copies of files on-site, creating mirror images of entire hard drives, or simply seizing the computers and reviewing their contents off-site.[5] Typically, the search warrant itself will specifically 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 it generally doesn't hurt to ask. If necessary, arrangements can usually be made to obtain electronic copies on an expedited basis after the search, in order to minimize the adverse impact on the company's operations.

Ask for split samples when agents seize samples, such as in environmental investigations. If a split sample is refused, take your own parallel sample (which you will probably wish to do under monitored circumstances once the agents have left the premises).

Advise the lead agent of any classified documents that are 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, the agency with jurisdiction over the information should be notified immediately.[6]

Advise employees not to discuss the search with others, except legal counsel.

4 Prosecutors and experienced agents will generally consent to such arrangements because they do not want their cases tainted by exposure to privileged materials. In addition, the DOJ Manual states that "a search warrant should normally not be used to obtain [attorney-client privileged or attorney work product] materials." Justice Manual § § 9-13.420 and 9-19.220.

5 The law regarding searches of computers and other electronic media is in flux. Searches (and the return) of seized computer hardware often takes weeks or months, although some courts are mandating shorter and more reasonable search periods.

6 Similarly, the agents should be advised if they confiscate any proprietary or trade secret information.

Detailed Guidance on Responding to a Subpoena, a Document Preservation Notice, or Other Government Process

A government-issued subpoena for documents, a document preservation notice, or other similar investigative demands, can raise a host of thorny issues, particularly for large or widespread companies which may possess huge amounts of documentary material, including electronically stored information ("ESI").

Companies have an affirmative duty to identify, locate, and maintain all information relevant to any known or foreseeable investigation and, later, to produce all non-privileged documents, including ESI, which are responsive to the subpoena or other form of process. It is critical to avoid the potential pitfalls in achieving compliance and, perhaps most importantly, to remain free of charges of obstruction.

- *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 or pending, or can be reasonably anticipated. The obstruction-of-justice provisions enacted as part of Sarbanes-Oxley make clear that a government investigation need not have commenced and a subpoena need not have been issued for the duty to preserve to arise: "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." 18 U.S.C. § 1519 (emphasis added).

- *Preservation – Hold Orders.* Once the duty to preserve arises, company counsel must move quickly to implement a "Hold Order" that tracks the government's information request (if available) to ensure that employees are on notice of the categories of information that must be held and preserved. The Hold Order should be drafted and issued as soon as possible. The potential consequences flowing from a post-duty loss or destruction of potential evidentiary material are too serious to sanction delay. The parameters of a Hold Order can always be expanded or modified as you learn more.

  A sample of a preliminary "Preservation Memo /Hold Order" is included at the end of this handbook. It can also be found at: http://www.crowell.com/PDF/Sample-Preservation-Memo-Hold-Order.pdf

- *Involve Outside Counsel as Soon as Possible.* As soon as possible, consult and coordinate with outside 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. It is beneficial to start those negotiations promptly.

Subpoenas for Testimony

If a company employee is served with a subpoena or other such notice to provide oral testimony (as opposed to merely directing the production of documents) in connection with a government investigation, you should immediately contact qualified counsel and email a copy of the subpoena to that counsel. The identity of the prosecutor or enforcement attorney handling the matter can often be determined from the face of the subpoena. In many cases, outside counsel can contact the prosecutor informally and obtain information regarding the subject matter of the proceedings and of the testimony and evidence being sought, and can advise accordingly.

Detailed Guidance on Responding to a Cyber Incident

Response and Investigation

Execute Incident Response Plan—
Preparation before an incident is critical.
A comprehensive incident response plan helps ensure you are taking reasonable steps to protect your sensitive data and you have a plan in place to aggressively respond in the event of an incident.

Engage Legal Counsel –
Once a cybersecurity incident has been identified, involve experienced legal counsel (in-house or external) as soon as possible to guide you through and direct the incident response process.

Retain Forensic Investigator –
A forensic investigator with incident response expertise will help determine the nature and scope of an incident, and can provide independent expert recommendations on remedial and preventive technical controls.
Having counsel retain and communicate with forensic investigators will help maintain confidentiality and privilege.

Review Insurance Policies –
Whether seeking coverage under a cyberinsurance policy or a traditional general liability policy, insurance can help to defray the high cost of a security incident. Review any applicable policies to determine what exactly is covered and identify what steps to take going forward in order to secure coverage, including timely notice to the carrier.

Identify Compromised Information –
With the assistance of your forensic investigator, identify what information has been compromised and the sensitivity of that information, and analyze the business impact of that loss.

Interactions with Government & Other Entities –
Evaluate the benefit of sharing information with third parties, including government entities and/or the appropriate Information Sharing & Analysis Organization (ISAO).

Notification

Determine Which Laws are Implicated –
Depending on the type of information involved, assess which laws and regulations apply to your industry:

- ✔ HIPPA
- ✔ Gramm-Leach-Biley Act
- ✔ State Breach Laws
- ✔ Critical Infrastructure Requirements
- ✔ Government Procurement Requirements
- ✔ FAR/DFARS, handling classified data
- ✔ FTC, FCC, SEC, CFPB, CFTC, etc.

Evaluate Notification Requirements –
Review the compromised information and evaluate relevant notifications (e.g., individuals, regulators, third parties via contractual requirements). Even if not mandated by state law, you may consider offering affected individuals free identity theft protection services. Identify call handling needs, either designating an individual or setting up a call center to answer calls and respond to questions regarding the incident.

Remediation

- Your forensic investigator, in coordination with counsel, may provide the company with a privileged final report and recommendation at the conclusion of the engagement. Implement recommendations for strengthening network security as soon as practicable to prevent a similar incident from occurring in the future.

- Conduct post-incident "lessons learned" analysis to review and, as needed, revise policies, procedures, and practices, as well as internal governance structure and information management. Review and assess internal governance structure for potential restructuring.

Following these guidelines will help support an efficient and effective security response process. Because preparation is a key factor in mitigating the impact of an incident, we also recommend that entities consider undertaking the following activities in advance to help ensure prompt and effective incident response: review insurance policies for coverage of incident-related issues; maintain a current, accurate, and accessible list of internal and external points of contact for incidents; regularly test your incident response plan and your incident response team by responding to hypothetical incident scenarios; prepare a tool kit with form notification letters and internal and external communications guidelines and sample scripts; identify potential outside counsel, forensic investigators, and other third-party incident response service providers to familiarize them with your organization, and vice versa.

Appendices & Links to Important "Crisis" Materials

Search Warrant Advice to Employees

Sample "Notice to Employees" for Search Warrants
http://www.crowell.com/PDF/Sample-Notice-to-Employees.pdf

Document Preservation

Sample "Preservation Memo/Hold Order"
http://www.crowell.com/PDF/Sample-Preservation-Memo-Hold-Order.pdf

Document Collection

Link to "E-Discovery in the Criminal Context"
http://www.crowell.com/documents/E-Discovery-in-the-Criminal-Context.pdf

Fact-Finding

Link to "Upjohn Warning: Recommended Best Practices When Corporate Counsel Interacts with Corporate Employees"
http://www.crowell.com/pdf/abaupjohntaskforcereport.pdf

Electronic Version

To download an electronic version of this crisis handbook, visit our website at
http://www.crowell.com/pdf/corporate-crisis-handbook.pdf

Sample Search Warrant Notice to Employees

CONFIDENTIAL

TO: All Employees

FROM: [Legal Counsel]

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.

First, it is important that no one remove or destroy any documents, papers, computer files, etc., while this investigation is pending. 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 [phone number].

Second, any requests by government agents for additional documents should be reported immediately to [legal counsel] at the above phone number and will be handled with counsel. Similarly, any requests for information or documents by news media should also be reported immediately to [legal counsel], who will handle such matters.

Finally, be aware that 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 do have the right to say you want 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, and by taking notes the attorney can minimize any misquoting of what you say. The company will arrange for an attorney to talk to you if that becomes necessary and you so desire. 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.

Sample Document Preservation Notice[1]

CONFIDENTIAL

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]

RE: Document Preservation Notice

Confidential Document Preservation Notice

This document preservation notice is strictly confidential should not be discussed outside of: (i) internal discussions necessary for document preservation and compliance; or (ii) communications with company counsel.

[For a purely internal investigation:]

An internal inquiry is being conducted by company counsel regarding [general description of subject matter 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 or deletion of such materials be suspended immediately.

[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 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]

[1] Please check with either Steve Byers (sbyers@crowell.com) or John Davis (jdavis@crowell.com) to ensure you have the latest version of this template if this version is dated more than six months ago.

Location and Form of Documents: 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 stored
  - In your office,
  - In common or shared storage areas,
  - At any other company facility,
  - In off-site storage facilities,
  - At your home; and
- Electronic documents stored
  - On company computer servers,
  - In company databases,
  - On company or personal desktop or laptop computers,
  - In company or personal email accounts,
  - In company or personal instant-messaging accounts,
  - In company or personal voice mail boxes,
  - On company or personal smart phones or tablets including text messages,
  - In company or personal cloud storage repositories,
  - On portable electronic media such as external hard drives, thumb drives or CDs.

Note. 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.

Meaning of "Documents": You must interpret the term "documents" broadly to include all types of hard-copy and electronic documents and data, including emails, instant messages, text messages, voice mail recordings, computer input or output, the contents of computer hard drives, and data in any other form in which data may be stored.

Other Instructions:

- These document preservation instructions take precedence over all other documents 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; in the cloud), and the automatic deletion or overwriting of data.
- 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.
- 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 me 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 [issuing attorney 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 relatedinquiry.

If you have any questions about these instructions, please call me at [issuing attorney phone number].

Thank you for your cooperation.

Sample Upjohn Warning

I am a lawyer for or from Corporation A. I represent only Corporation A, and I do not represent you personally.

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

Your communications with me are protected by the attorney-client privilege. But the attorney-client privilege belongs solely to Corporation A, not you. That means that Corporation A alone may elect to waive the attorney- client privilege and reveal our discussion to third parties. Corporation A alone may decide to waive the privilege and disclose this discussion to such third parties as federal or state agencies, at its sole discretion, and without notifying you.

In order for this discussion to be subject to the privilege, it must be kept in confidence. In other words, with the exception of your own attorney, you may not disclose the substance of this interview to any third party, including other employees or anyone outside of the company. You may discuss the facts of what happened but you may not discuss this discussion.

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

Notes

Notes

Crowell & Moring LLP is an international law firm with offices in the United States, Europe, MENA, and Asia that represents clients in litigation and arbitration, regulatory and policy, and transactional and corporate matters. The firm is internationally recognized for its representation of Fortune 500 companies in high-stakes litigation and government-facing matters, as well as its ongoing commitment to pro bono service and diversity, equity, and inclusion.

crowell.com