BUSINESS EMAIL COMPROMISE EVENT

Stage 1: Identify-Report-Engage

Because you are reading this, it's likely that Lewis Brisbois has already sent you an engagement letter. You are always our priority, even before we are engaged. If there are any questions we can answer now, please do not hesitate to reach out.

Identify: Someone at your company discovers the company may have fallen victim to a Business Email Compromise (BEC) attack. A BEC attack generally occurs when a **"threat actor"** spoofs or illegitimately accesses email accounts to impersonate senior executives, customers, or outside vendors in emails scams designed to trick employees into wiring payments or making purchases under fraudulent pretext. Typically, you observe suspicious emails requesting "urgent" action or a change in payment information or have discovered that a payment has been made to an incorrect account.

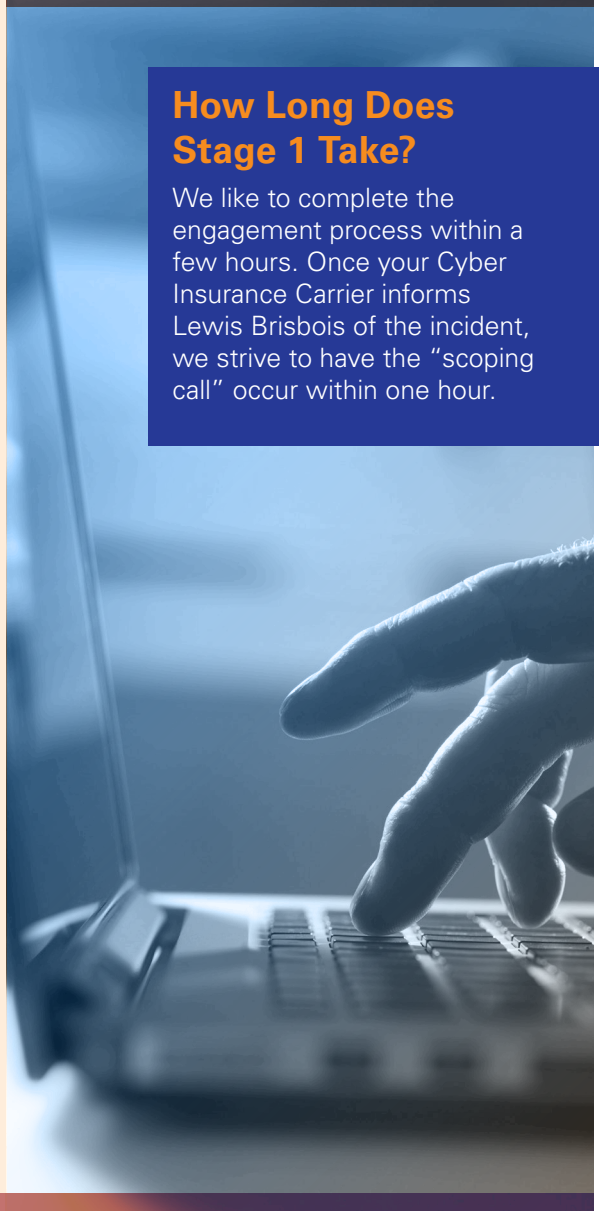
Report: Once the BEC attack has been identified, someone at the company informs the company's Cyber Insurance Broker, Cyber Insurance Carrier, or both.

Engage: Your company's Cyber Insurance Carrier contacts Lewis Brisbois.

1. **Initial Email/Call.** Lewis Brisbois/Your Cyber Insurance Carrier will contact you to schedule a **"scoping call."**
2. **Scoping Call.** During that call, usually with a trusted forensic investigation company, we will ask you: (1) specific questions about the incident; and (2) general questions about your company's environment, so it is helpful to have someone knowledgeable about both on the call.
3. **Engagement Materials.** After the scoping call, Lewis Brisbois will send its engagement letter and the forensic firm's engagement materials. **Importantly, Lewis Brisbois will engage the forensic investigator on your behalf to bolster an argument that the investigation and related forensic findings are privileged. This is critical in preventing information relating to the incident from being disclosed or used in subsequent legal proceedings.** Once the engagement materials are signed, the investigation is ready to begin. Lewis Brisbois will get the requisite approvals from your Cyber Insurance Carrier (i.e., ensure the cost of the legal services and forensic firm services are covered under your cyber insurance policy, subject to any applicable retention or policy limit of course) before sending the engagement materials to you.

How Long Does Stage 1 Take?

We like to complete the engagement process within a few hours. Once your Cyber Insurance Carrier informs Lewis Brisbois of the incident, we strive to have the "scoping call" occur within one hour.



BUSINESS EMAIL COMPROMISE EVENT

Stage 2: Recover-Contain-Collect-Restore

At Lewis Brisbois, we have a single objective for each engagement: To minimize the impact of the incident on the company. In BEC attacks, this involves not only **recovering** lost funds, but **containing** the incident to prevent further damage.

1. **Recovering Lost Funds.** Unfortunately, many companies do not realize that they have experienced a BEC attack until funds have been lost. Recovering lost funds may be difficult if too much time has passed since the payment was made. Thus, all organizations should contact the originating financial institution to request a recall or reversal as soon as possible, and notify law enforcement (i.e., FBI or the United States Secret Service) immediately. The FBI and Secret Service are often able to recover lost funds if they are notified within 48-hours of the payment. Lewis Brisbois has extensive relationships with law enforcement and can facilitate these discussions. Remember, communications with banks and law enforcement are not privileged; thus, it is important to exercise caution when providing these notifications.

2. **Contain. "Stop the Spread."** It is important to contain the spread and scope of the incident and eradicate the threat actor from your environment. Containment comes in many forms. For instance, you may have unknowingly begun the process when you changed/reset passwords for the impacted accounts.

But containment, is only part of the process.

We also want to answer three main questions:

DID THE THREAT ACTOR ENTER YOUR NETWORK?

WHAT FILES/FOLDERS DID THE THREAT ACTOR ACCESS ONCE IN YOUR NETWORK?

WHAT FILES/FOLDERS, IF ANY, DID THE THREAT ACTOR TAKE FROM YOUR ENVIRONMENT?

To answer these questions, we usually need a forensic vendor to collect evidence to analyze.

3. **Collect.** If a forensic investigation is needed, the forensic vendor will collect forensic evidence. The forensic evidence collected will vary based on your environment and what is available, but it may include: firewall logs, user logs images of servers/workstations, or actual hard drives.

You should preserve all logs once you detect an incident.

We know what you are thinking; we want to restore operations and get back-to-business. We get it and we want that too. But we must ensure that the threat is fully removed from the environment before moving forward. Not doing so could result in the threat attacker still maintaining a foothold in your systems, which could result in another data security incident.

4. **Restore**. In BEC attacks, "restoration" may not always be needed. If any accounts or systems were suspended because of the incident, however, this is when we can get them back up and running. Sometimes a company may elect to migrate its email to the cloud, so the environment is "new" and "clean."

How Long Does Stage 2 Take?

This Stage can take days, usually weeks, but possibly months. The time depends on many factors, including the: (i) email provider (ii) availability of logs; (iii) number of suspected email accounts at issue; and (iv) amount and type of forensic evidence available.

BUSINESS EMAIL COMPROMISE EVENT

Stage 3: Analyze and Assess

In the **Analyze and Assess** stage, the company starts to get answers to questions. Typically, at this stage, the company learns things such as the **"root point of compromise"** and the scope of **"data access/ exfiltration."**

1. **Analyze Forensic Findings.** Once the forensic company has collected and analyzed the forensic evidence, it is ready to present its findings. Generally, a forensic investigation seeks to answer *how the* threat actor entered the company's network (root point of compromise) and *what the* threat actor did once in the environment. Depending on the forensic findings, the company may gain insight into ways to reduce the likelihood of an incident happening again.
2. **Assess Resulting Legal Obligations.** Once the forensic findings are presented, Lewis Brisbois assess what legal obligations are triggered by the data security incident (i.e., did a **"data breach"** occur). Depending on if the threat actor has accessed or exfiltrated files and the content of those files, the company may have to undergo **"data mining"** to help identify the scope of **"personal information"** that was accessed or acquired.

How Long Does Stage 3 Take?

Once the forensic findings are finalized, Lewis Brisbois typically identifies the resulting legal obligation within days.

Stage 4: Act on Forensic and Legal Findings

In the **Act** stage, the company takes steps to comply with any legal or regulatory notification obligations. The company may also implement additional security measures depending on the forensic findings to reduce the likelihood of this type of incident from recurring. Depending on the forensic findings, Lewis Brisbois will advise whether a **"forensic report"** is recommended.

Once notifications are complete and/or there are no further actions to take, Lewis Brisbois will prepare a "Matter Summary" for your records. The Matter Summary will memorialize the findings and resulting legal conclusions from the data security incident. We recommend keeping this document for a minimum of 5 years, out of an abundance of caution.

How Long Does Stage 4 Take?

Once Lewis Brisbois receives the information needed to provide the required notifications (e.g., names of impacted consumers, data elements at issue, addresses for impacted consumers, etc.), the notification process can take days, sometimes weeks. If needed, Lewis Brisbois will partner with vendors who assist with mailing/notifications to streamline this process.

BUSINESS EMAIL COMPROMISE EVENT

FAQs

Stage 1 Identify-Report-Engage

Q. Should I even report the data security incident to my broker/carrier?

A. Yes. It is better to report out of an abundance of caution. So, if you are unsure, err on the side of caution. If it turns out to be a situation that does not require forensic or legal investigation, Lewis Brisbois will tell you, at no charge. So other than taking the time to call us and ask, "over-reporting" won't cost you anything.

Q. Do I need to engage Lewis Brisbois? After all, this is an IT/security issue.

A. Yes, you should. Whether it is Lewis Brisbois or another law firm (we hope it is us), we strongly recommend engaging legal counsel to assist with the incident response process. First, doing so will bolster an argument that the investigation, findings, and related discussions are privileged. But that is not the only reason why. At Lewis Brisbois, we have led hundreds of organizations through the incident response process, so we know what to expect and when. We also understand the emotional impact data security incidents can have on organizations and their employees - the organization's most important asset. Our experience allows us to bring calmness, clarity, and a clear path forward at a time when things feel uncertain.

Q. What is "privilege"?

A. The attorney–client privilege and the work product doctrine are two related but distinct doctrines to protect information that is shared with legal counsel from future disclosure. The attorney–client privilege protects communications to and from one's attorney(s) (and their delegates) for the purpose of seeking legal advice, while the work product doctrine protects materials prepared by an attorney — or the agents of an attorney — in anticipation of litigation. In the context of data security investigations, these two protections often overlap. Some people tend to group them together and treat them interchangeably, but the distinct purposes, origins, and tests for these two protections inform the unique methods that must be employed to assert them during the life of the investigation and any subsequent litigation.

Q. Why does privilege matter?

A. Unfortunately, the information companies discover during data security incidents are: (i) needed to contain the incident and prevent it from recurring but (ii) may be used against the company should litigation or a regulatory investigation ensue (e.g., plaintiffs may use a forensic report as "evidence" that a company failed to maintain reasonable security procedures). Thus, taking steps to prevent the disclosure of this information is critical. The pitfalls of failing to consider these protections can be drastic, but they are often slow to emerge, sometimes taking years to fully develop. By the time it is apparent that steps were not taken to preserve protections, it is often far too late to rectify the situation.

Q. Do you represent me or the Cyber Insurance Carrier?

A. You. Lewis Brisbois represents the company, not the Cyber Insurance Carrier. Your Cyber Insurance Carrier has vetted us and recommends our legal services for its insureds, like you. But we represent you.

BUSINESS EMAIL COMPROMISE EVENT

FAQs

Q. Are these costs covered by our cyber insurance?

A. Generally, yes. At Lewis Brisbois we obtain approval from your Cyber Insurance Carrier before performing any services or engaging any third-party vendors on your behalf. We will let you know that a service has been pre-approved by your Cyber Insurance Carrier so there are not surprise costs. Of course, any insurance approval is contingent on satisfaction of your SIR (self-insured retention amount) and applicable policy limits.

Q. Who pays the costs of the incident response?

A. It depends. Cyber insurance policies differ. Usually, your Cyber Insurance Carrier will pay the invoices (legal, forensic, third-party vendors) once the company has satisfied its SIR (self-insured retention amount).

Stage 2 Recover-Contain-Collect-Restore

Q. Our company has already conducted an internal investigation, why should we engage a forensic vendor to do the same thing?

A. Several reasons. First, it can be useful to have an independent, third-party investigate. Often, the internal team conducting the investigation is the same team responsible for protecting the company's IT systems and assets. Bringing in a third party removes the possibility (or even just optics) of any bias. Second, because Lewis Brisbois engages the forensic firm, there is a greater likelihood that the investigation will be protected under attorney-client privilege.

Q. Do I need to tell law enforcement?

A. It depends. If you have submitted payment to an incorrect account, we suggest contacting law enforcement immediately. The FBI and Secret Service are often able to recover lost funds if they are notified within 48-hours of the payment. Lewis Brisbois has extensive relationships with law enforcement and can facilitate these discussions. Remember, communications with law enforcement are not privileged. Thus, it is important to exercise caution when providing these notifications. There are other benefits to notifying law enforcement too, especially if you need to report the incident to consumers or regulators. From an optics perspective, this is always a good step to take, even if law enforcement does not act on the case (which is often the case).

Stage 3 Analyze-Assess

Q. When do I have to notify?

A. It depends on the type of information that was accessed or acquired and the contents of that information. Generally, only data security incidents that impact "personal information" will trigger any notification requirements. What constitutes "personal information" varies depending on the applicable federal and state data breach notification laws.

Q. Should I ask for a forensic report?

A. It depends on the event and the surrounding circumstances. Lewis Brisbois will advise on whether a forensic report is recommended.

BUSINESS EMAIL COMPROMISE EVENT

FAQs

Q. Should I share the forensic report with my customers or any other third parties?

A. No. That will waive any applicable attorney-client privilege covering the report. But at Lewis Brisbois we can help you report findings to your customers without providing them with a privileged report.

Stage 4 Act on Forensic and Legal Findings

Q. If I must notify consumers, will Lewis Brisbois help me?

A. Of course. Lewis Brisbois will prepare the consumer notification materials for your company. We will also arrange to have the notices mailed, set-up a call-center for notice recipients to contact with questions and assist with obtaining credit monitoring, if needed.

Q. What about notifying regulators?

A. Lewis Brisbois will identify any regulators that require notification and will notify them too.

Q. I want to tell my employees/customers about the event before they receive a letter. Can you help?

A. Yes. If it is in your best interests to do so, we can help prepare responses and escalations guides to commonly asked questions, internal messaging to employees and leadership, external messaging to customers and vendors, messaging to post on your company website, and responses to media inquiries.

Q. Will my insurance cover notification costs?

A. Generally, yes. At Lewis Brisbois we obtain approval from your Cyber Insurance Carrier before performing any services or engaging any third-party vendors on your behalf. We will let you know that a service has been pre-approved by your Cyber Insurance Carrier so there are not surprise costs. Of course, any insurance approval is contingent on satisfaction of your SIR (self-insured retention amount) and applicable policy limits.

BUSINESS EMAIL COMPROMISE EVENT

Glossary

1. **Data Access:** Occurs if the threat actor viewed data/documents while in your environment.

2. **Data Breach.** While the definition of "data breach" varies by the applicable federal and state data breach notification laws, data breaches are generally defined as the unauthorized access and/or acquisition of personal information. Generally, only "data breaches" trigger reporting obligations.

3. **Data Mining:** A two-step process. In step one, a third-party vendor "mines" the data impacted by the data security incident, which means that they run a series of search terms across the data. In step two, the third-party vendor "reviews" the data resulting from the search and creates a spreadsheet that identifies the name, address, and categories of information belonging to each individual potentially impacted by the data security incident.

4. **Exfiltration:** The act of a threat actor taking or stealing data/documents from your environment.

5. **Forensic Report:** A final report prepared by the third-party forensic investigator at the direction of Lewis Brisbois, detailing the findings from the investigation, including the root point of compromise, and any unauthorized access/exfiltration of information.

6. **Personal Information:** The definition of "personal information" varies based on the applicable federal and state data breach notification laws. At a high-level, however, almost all statutes consider the following types of information to be personal information when not encrypted:

    a. An individual's first name or first initial with last name combined with one or more of the following date elements:

        i. Social Security number

        ii. Driver's license or identification card number

        iii. Account number, credit card or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account

7. **Root Point of Compromise:** How the threat actor got into your environment.

8. **Scoping Call:** The initial call during with Lewis Brisbois and the forensic vendor obtain information about the BEC, ask questions about the company's environment, and use that information to "scope" the extent and cost of the investigation.

9. **Threat Actor:** The actor(s) that illegitimately entered your environment.