RANSOMWARE EVENT

Stage 1: Identify-Report-Engage

Because you are reading this, you have likely already identified and reported a data security incident. So why not go ahead and engage?

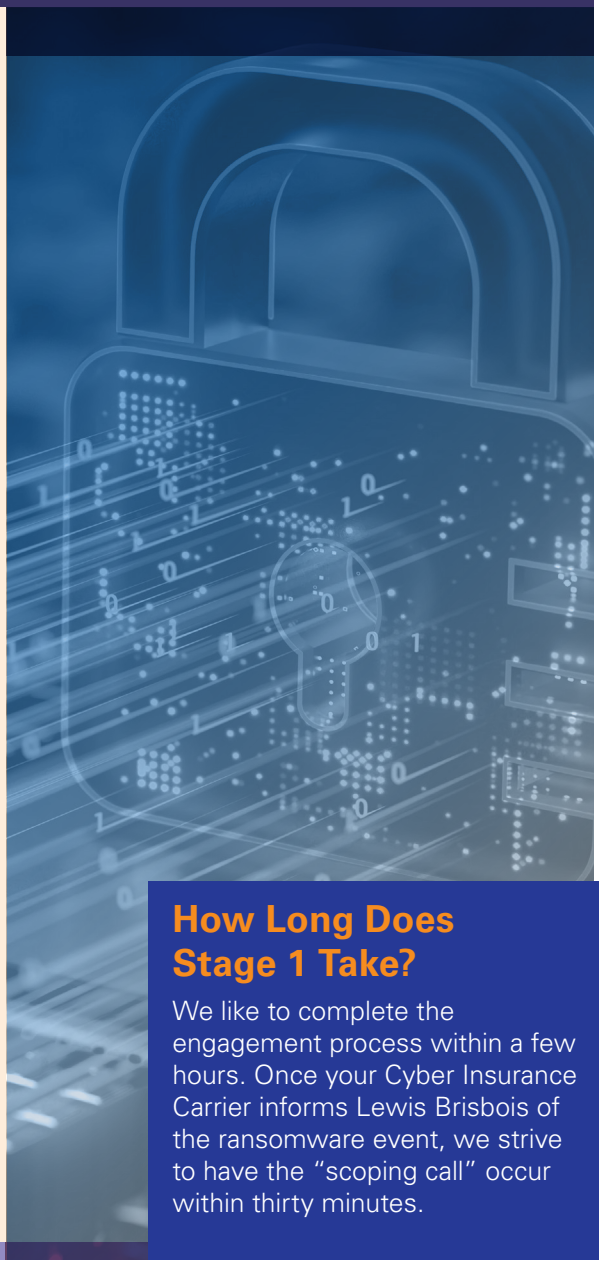
Identify: Someone at your company discovers a ransomware attack. A ransomware event generally occurs when a **"threat actor"** enters the environment and encrypts company servers and workstations. Typically, you observe network encryption or a ransom note.

Report: Once the ransomware event has been identified, someone 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 ransomware event; 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.

You have enough to worry about.
Let us worry about insurance approvals.



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 ransomware event, we strive to have the "scoping call" occur within thirty minutes.

RANSOMWARE EVENT

Stage 2: Contain-Collect-Remediate-Restore

At Lewis Brisbois, we have a single objective for each engagement: To minimize the impact of the incident on the company. To achieve this objective, we want to first contain the ransomware event.

1. **Contain. "Stop the Spread."** It is important to contain the spread and scope of the ransomware event. Containment comes in many forms. For instance, you may have unknowingly begun the containment process when you disconnected/disabled Internet access to your servers/workstations to limit the spread of a ransomware attack.

But containment is only part of the process.

We also want to answer three main questions:

HOW 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.

2. **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 make sure the environment is remediated first.

3. **Remediate.** Before we can restore business operations, we must ensure that the threat has been remediated (i.e., the threat no longer exists). Remediation often includes deploying an EDR Tool (end-point-detection-and-response tool) across your environment.

Once the environment has been remediated, restoration can begin. Sometimes restoration can occur piecemeal; sometimes restoration can occur in tandem with collection and remediation. Sometimes, restoration must wait until the end of Stage 2.

4. **Restore**. Sometimes a company can restore from backups or recreate lost or damaged information from other sources. Sometimes, a company must rely on a threat actor to obtain a decryptor key to unencrypt servers/workstations before restoring.

How Long Does Stage 2 Take?

This Stage can take days, sometimes weeks, and possibly months. The time depends on many factors, including the: (i) scope of encryption (ii) status of backups; (iii) amount and type of forensic evidence available; and (iv) whether a company needs to obtain a decryptor.

RANSOMWARE 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 determines what legal obligations, if any, 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 satisfies 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.

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.

RANSOMWARE EVENT

Threat Actor Negotiations

After a threat actor deploys ransomware on a company, the threat actor leaves a ransom note. Sometimes a company has no choice but to contact the threat actor to obtain a key that will decrypt the company's encrypted environment. At Lewis Brisbois, we partner with threat actor negotiation experts that communicate with the threat actor for us. If we need to pay the threat actor, we have trusted experts that will facilitate the payment too.

Sometimes a company has choices. It may not need a decryptor. We can advise the impacted company throughout the threat actor communication process – provide an overview of the steps of the process, strategy on negotiation timing and amount, and how payment or non-payment may impact the company.

Never contact the threat actor on your own.
Leave this to the experts.

RANSOMWARE 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 thousands 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.

RANSOMWARE 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 no 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 Contain-Collect-Remediate-Restore

Q. If resuming operations is so important, why do we collect information before we restore?

A. The goal is to minimize the impact on the organization. If we restore too soon (before containment), then we risk restoring the company on a contaminated network. And if we restore before we collect, we risk reducing/destroying forensic evidence that helps us understand how the threat actor entered the environment.

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 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. Sometimes your cyber insurance may require you to notify the FBI before paying a ransom to a threat actor. Even if your cyber policy does not require it, it is good practice to notify the FBI before making any ransom payment. There are other benefits to notifying law enforcement too.

Q. Should we contact the threat actor?

A. Not without our assistance.

Q. Is it illegal to pay a ransom?

A. Generally, no. Some states have laws now prohibiting local government agencies from paying a ransom, but that is the exception. Before paying a ransom, an expert team will complete an OFAC check to make sure that the threat actor being paid is not a sanctioned individual or entity as payment to a sanctioned individual or entity is a violation of U.S. laws.

Q. What guarantee do I have that the threat actor will deliver a decryptor after payment?

A. There are no guarantees. We have access to data trends, so we know which threat actor groups tend to deliver decryption keys.

RANSOMWARE EVENT

FAQs

Stage 3 Analyze-Assess

Q. When do I have to notify?

A. You may not. It depends on the type of information that was accessed or acquired and the contents of that information.

Q. Should I ask for a forensic report?

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

Q. Should I share the forensic report with my customers?

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 provide 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.

RANSOMWARE EVENT

Glossary

1. **Data Access:** The viewing of data/documents by a threat actor 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 taking of data/documents by a threat actor 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 with Lewis Brisbois and the forensic vendor to obtain information about the ransomware event, ask questions about the company's environment, and use that information to "scope" the extent and cost of the investigation.

9. **Threat Actor:** The ransomware actor(s) that attacked your environment.