# INCIDENT RESPONSE

## You Experienced a Data Security Incident, Now What?
An Overview of the Incident Response Process

## The Lewis Brisbois Difference

A data security incident often creates uncertainty for the impacted company. There are business uncertainties: How soon can we resume normal operations? What should we say to our clients and customers? There are IT uncertainties: How did this happen? Is this our fault? There are legal uncertainties: Who do we need to notify? Will we be sued or fined? And a host of others: Do we need to notify law enforcement? When?

At Lewis Brisbois, we understand these operational and sometimes, emotional, uncertainties. We have led hundreds of organizations through the incident response process, spanning all types of data security incidents – ranging from a lost laptop through a ransomware attack that places an organization on the brink of collapse – and everything in between.

Because we are attorneys, we of course provide companies with legal advice through the incident response process by identifying the company's legal obligations resulting from the data security incident, if any, and ensuring compliance with them. But that's not all we do. We are your partners, your advocates, your trusted advisors, and most importantly, your go-tos during and after the incident response process.

We understand that many companies have never gone through the incident response process. So, we leverage our experience and the relationships we have cultivated over the years with forensic vendors, law enforcement, and other critical partners, we lead them through it.

We will: (i) let you know what to expect to minimize surprises and help you manage expectations both internally and externally; (ii) help throughout the incident response process and inform your employees and customers about the incident so you know what to say to them and when; (iii) help you when you have to make time-sensitive decisions so you can minimize the incident's impact on your company; (iv) partner you with trusted experts and advisors to help ensure that the incident is contained so you resume operations as expeditiously, yet safely, as possible; and (v) provide timely updates to your Cyber Insurance Carrier on your behalf so that is one less thing you need to worry about.

**Our goal is not to simply restore the organization to status quo after the data security incident; we want the organization to be in a better position after it.**

# INCIDENT RESPONSE

## Overview of the Incident Response Process

At Lewis Brisbois, we view the incident response process as a four-stage-process. While what happens during each stage will of course vary based on the incident, each incident generally follows these four steps.

## GENERAL PROCESS

### STEP 1

### IDENTIFY-REPORT-ENGAGE

- Scoping Call
- Review & Sign Engagement Materials

### STEP 2

### RECOVER-CONTAIN-COLLECT-RESTORE

- Attempt to Recover Lost Funds
- Kick-off Forensic Call
- Periodic Forensic Calls

### STEP 3

### ANALYZE-ASSESS

- Final Forensics Call
- Analyze Forensic Findings
- Assess Legal Obligations
- Data Mining/ Manual Review

### STEP 4

### ACT ON FORENSIC AND LEGAL FINDINGS

- Prepare/ Send Legal Notifications
- Implement Additional Security Measure, If Needed