2016 HOSPITALITY LAW CONFERENCE

TED TALK: DATA SECURITY INCIDENT RESPONSE PLANS

"Time is money." That idiom is as true as ever when it comes to responding to a data security incident that has affected your company. Planning and preparedness leads to a faster, more organized and more effective response, which in turn reduces exposure and potential liability from a number of perspectives.

How can you ensure that all of this will occur quickly when a data incident occurs? The answer is by having a thoughtful, thorough and rehearsed data incident response plan at the ready.

A quick response is key in reducing the cost and pain of a data breach incident.

Studies by experts in the security industry have tended to show that a the speed with which a company responds to a data security incident is directly linked to the amount of time, energy and money they expend in response tasks. Lack of planning and preparedness slows reaction time, which in turn increases the possibility of consequences to a company that could have been avoided.

1. A fast forensic investigation allows companies to identify and close security weaknesses and to quickly understand the nature and scope of the information that may have been compromised. Many electronic intrusions may be continuing even after the breach is initially detected, because the malware and system activities of the intruders are well disguised. Your forensic assessment professionals can identify and shut off continuing data compromise to close the window on the amount of data potentially affected.

2. Efficient and controlled internal and external communications help to preserve your company's reputation. Data breach incidents often prompt the interest of the media,

regulatory agencies and those who believe their data may have been compromised. Quickly controlling the message about the incident, both internally and externally, helps convey that your company is taking the matter seriously and acting expeditiously to mitigate harm that may flow from the incident.

3. Prompt legal analysis and advice may help to eliminate or limit regulatory investigations and ensure timely notification to affected individuals. Data breach notification laws are increasingly featuring tight time limitations for notifying affected individuals and regulators. Knowing your duties and executing them properly helps to reduce the likelihood of private lawsuits and regulatory investigations and enforcement actions.

What should be in your company's data incident response plan?

IDENTIFY YOUR INCIDENT RESPONSE TEAM. The right people must be leading the incident response effort, so "job one" is identifying who those people are and getting them to understand their roles. Your team should include, at a minimum:

- A highly-placed corporate team leader
- Your top legal officer and outside data breach response counsel
- Your chief security/privacy officer, if applicable
- To the extent that the incident involves electronically stored information, your chief information systems officer
- Your communications leader
- Your risk management department

In addition to the foregoing, your plan could identify a pre-selected outside forensic investigation firm, and outside public relations/communications firm, and a law enforcement contact at both the state and federal level.

ESTABLISH YOUR INCIDENT RESPONSE PROCEDURE.

For starters, someone must be in charge of knowing who the members of the Incident Response Team are and how to contact them at all times. The Team members should know where they will meet if alerted to an incident. In order for the Incident Response Plan to be fully effective, it should be practiced, and drills should occur on a regular basis.

Once the Team is assembled, they should generally execute upon the following tasks, roughly in this order:

- Confirm the incident and source. For this step, if the breach is electronic in nature, your IT department representative should be consulted for all known details. If appropriate, your forensic investigation vendor should be contacted and brought in promptly to begin its investigation and analysis. It is typically good policy to report the incident to law enforcement, and document that you have made such a report. Cyber intrusion and information theft are crimes.
- Identify cause, preserve evidence. The forensic investigation firm will often image the drives of the affected systems so as to preserve evidence of the intrusion while enabling the investigator to perform its analysis. They may advise the company to take certain systems offline pending a more certain identification of the cause and status of the attack. Logs should be carefully preserved.
- Remediate. Malware must be removed and security gaps closed. At this time, a determination should be made as to what information was exposed, whether the nature of the information triggers any legal duties or business concerns, and the likelihood that the information could be used for the commission of identity theft, fraud, corporate extortion or theft of trade secrets. A determination should be made as to whether credit

monitoring/fraud protection/restoration services will be offered to affected people at the company's cost. This is now mandated in a few states, and others are considering following suit.

- Communications plan (internal, external). Your corporate team leader should work with the legal team and communications team to formulate the company's message regarding the incident. Know what you want to say to the media, to members of the public, and to those who believe that their personal information may have been compromised in your incident. Talking points may be formulated, as well as a press release. Inquiries from law enforcement investigator and government regulatory agencies should be immediately referred to inside or outside counsel for handling.
- Notification – affected persons, regulators. When a breach occurs, in the vast majority of cases, notification of affected persons is controlled by federal or state statute. Your legal team should provide an analysis and recommendations concerning: (a) who should be formally notified; (b) the content and method of the notification; (c) the timing of the notification; and, (d) whether regulators must also be notified, and if so, the content and timing of those notifications.
- Internal reporting. Response is going to take several weeks and possibly months. The Team should meet regularly to review the status and response tasks. Those charged with particular tasks should report on progress or problems.
- Ideally ….. Closure. At a certain point, the company has done everything it can to respond. If there are no ongoing investigations, class actions lawsuits or credit card industry fraud cost recovery actions pending, and enough time has passed, the company

may close its file on the incident. However, based upon the facts learned, a final assessment should be made as to whether improvements in security are warranted.