2019 Annual Conference
March 13 -15 2019
Orlando, FL

Cyber Liability and Data Privacy – A Public Entity Perspective

I. Public Entity Data Breaches

Recent Public Entity Data Breach Cases

On March 12, 2018, a California Department of Public Health (CDPH) contractor tasked with performing health facilities inspections had some documents and a laptop stolen from his vehicle. The laptop contained data with first and last names, date of birth, social security numbers, addresses, diagnoses and other health information, health insurance information and demographic information. Under Cal. Civ. Code § 1798.29 and § 1798.82, notification to the California Attorney General's Office is only required in the event that more than 500 records were breached. The CDPH did not provide an estimate of the number of breached records in the notification letter of May 23, 2018.

On July 3, 2018, the Advanced Law Enforcement Rapid Response Training center at Texas State University disclosed that a data breach had exposed the personal data of thousands of local, state and federal law enforcement officials who had applied for or received active shooter response training over the past few years. The data cache contained information up to April 2017 and was uploaded about one year later to a web server at the training center, without password protection. The database has since been removed, but it is not clear whether access to that database was monitored or logged. Under Tex. Bus & Com § 521.053 ("Notification required following breach of security of computerized data"), the training center is not required to provide a notification letter to the Texas Attorney General's office, but is required to provide notice of this breach to every individual included in that database within 48 hours. Under Tex. Gov't Code § 2054.1125 (b) (1), all Texas state agencies must also comply with this requirement.

Whether by accident, negligence or intent, unauthorized access to computer data is increasingly common, with new data security breaches being reported nearly every week. Most of these breaches can be avoided or limited by using a few basic data security practices, starting with taking inventory of just what sensitive information your organization is storing, and where, determining whether such information is truly necessary for the operations, and either securing it if it is needed or destroying it if it is not. Similarly, think about where and how you access the Internet, since anywhere you can reach out from could also serve as a channel for someone else to reach in to you and yours.

TAO Autobus Orlando - Hypothetical

To better illustrate and experience the cyber liability issues surrounding a data breach, we have constructed a scenario using a hypothetical company named "TAO Autobus Orlando", a self-driving tour bus company contracted by the City of Orlando to respond to information kiosks that the City maintains at transportation hubs and specific areas of interest. These kiosks call a TAO Mini Bus, which otherwise would tour through a series of preset stops with a pre-recorded tour information message playing in the background.

This is patterned after the Local Motors "Olli" 12-passenger self-driving minibus that was used at the July 2018 Annual Meeting of the Northeast Association of State Transportation Officials ("NASTO") in National Harbor, Maryland to transport attendees to and from the Local Motors facility that was hosting a conference panel.

In this hypothetical, there will be a minibus vehicular accident which gets traced back to a series of network intrusions. The session attendees will be designated the Data Breach Response Team, with different areas anchored by the session panelists, and the hotel itself designated as the main offices of TAO Autobus Orlando.

II. Autonomous Vehicle Operations

Data Security and Privacy in Operations and Communications

(Based on material provided by Kellie Howard-Goudy, Esq.)

The first segment of the breach response briefing will be a review of data security and privacy concerns in autonomous vehicle operations and communications. In addition to having a general road map overlay that the autonomous vehicle ("AV") operates within,

there will be Vehicle-to-Vehicle ("V2V") communications for V2V-enabled vehicles to better coordinate traffic flow, as well as potentially Vehicle-to-Everything ("V2X") communications that would enable V2X-enabled traffic control systems to notify the AV of applicable traffic signal changes, speed limits and known road hazards. This would be in addition to the built-in video and lidar sensor arrays aboard the vehicle, and any coordination the onboard AV systems would maintain with a centralized computer processing center (which would likely maintain a current version of the road map with hazards, obstructions, and emplacement of other V2V and V2X vehicles, as well as the notification and routing systems tied into the City of Orlando information kiosks by which the TAO vehicles are summoned.

While all such data communications would need to be encrypted, the possibility exists that such communications encryptions may be compromised. Additionally, all the data communication centers, such as other cars, traffic control systems, and centralized computers could themselves become compromised by network intrusion, with operational data potentially altered or individual's private information accessed.

The Breach Response team will be notified that a network intrusion is highly likely at this time, and to stay off the computer network.

Insurance Claims Analysis

One of the primary concerns with insuring autonomous vehicle operations lies in the broad scope covered by this new technology. Would a vehicular collision be covered as an auto collision claim, a products liability claim, and/or a cyber liability claim? The panelists will discuss insurance such coverage issues, inviting participation from attendees as we explore this new area of insurance claims.

III. Data Breach Response

Roles and goals of the Breach Response Team members

For this session, the TAO Breach Response Team will be nominally separated into five main areas:

- Information Technology ("IT")
- Operations ("Ops")
- Management, including Finance and Public Relations
- Legal Counsel

- Representatives from City of Orlando and service providers ("Reps")

The IT folks will be concerned with mobilizing the data forensics team, preserving the computer systems as best they can, and freezing operations until any intrusion has been blocked and the damage assessed and remediated. The Ops folks will be concerned with resuming operations, despite the best efforts of the IT folks. Management will be mediating between Ops and IT while doing damage control with their customers (City of Orlando in particular). Legal Counsel will be pursuing regulatory compliance as well as advising on the potential liability risks of proposed actions by IT, Ops and Management. The Reps will want to be generally helpful without admitting any fault or liability, and will likely be seeking waivers of liability in the pursuit of facilitating computer forensics and remediation efforts by TAO's IT folks and their data forensics team.

We will note that this is a simplified view for purposes of this tabletop exercise, and that the specific composition of an insured's data breach response team will depend on the nature of their operations. We will also note that experience counts, and that the level of sheer panic will be reduced if the data breach response team meets and drills regularly across a variety of potential scenarios.

At this point in the presentation, the panelists will seek out any session attendees who have a smartphone, laptop or other electronic device connected to the hotel's WiFi network. They will then be informed that a Remote Access Trojan ("RAT") malware packet was downloaded into their devices, that all contents of those devices have since been uploaded to an outside location by the attackers, and that their devices are now part of the "crime scene."

This will emphasize that a data breach can result from common habits, and that an attorney (for instance) may have his or her laptop preset to log into a client's corporate WiFi network if they visit that client regularly… and that they too can become part of the data breach when the laptop is powered up.

Data breach reporting requirements

As of now, all 50 states of the U.S. required data breach notification for unauthorized disclosure of personally-identifiable information and private health information. Of those, at least 23 states (including California and Florida) also required that the state attorney general's office be notified as well, although some of these states have set a

threshold (typically either when 500 or 1,000 persons were affected) before mandating notice to that state's attorney general.

A number of these states also maintain separate breach notification statutes for state and local agencies or other public entities, although many do not distinguish significantly between the reporting requirements between public vs. private entities. In California, Cal. Civ. Code § 1798.29 governs state agencies, while Cal. Civ. Code § 1798.82 governs persons or businesses that conduct business in California. In Florida, 501.171 Fla. Stat. (2018) combines both public and private entity regulation into a single statute. In Texas, Tex. Bus. & Com. § 521.053 governs notification by persons and businesses, while Tex. Gov't Code § 2054.1125 covers state agencies, primarily by referencing the statute for persons and businesses.
While California and Florida both mandate notice to the State Attorney General's Office of a security breach, Texas does not. Florida's AG notification threshold starts at 500 or more, while California requires more than 500 (501 or more).

Each state has its own statutes covering data privacy law and security breach notification standards. Such statutes should be consulted on a state-by-state basis for compliance in the event of a data security breach.

Confluence of regulatory efforts on data privacy and cyber liability

(by Barry Miller, Esq.)

Recently, a confluence of regulatory efforts on cyber security matters from separate quarters may potentially affect the insurer/attorney relationship.

The National Association of Insurance Commissioners passed a model cyber statute at the end of 2017 that has since been adopted by South Carolina, and is being considered in other state legislatures. This model act requires insurers to take steps to protect electronic information, and requires them to make sure that their vendors, including defense counsel, to the same.

The Restatement of the Law of Liability also has provisions that would make an insurer liable for defense counsel's malpractice.

Rule 1.1 of American Bar Association Model Ethics Rules requires competence from attorneys, however its comments now define "competence" to include a requirement that attorneys keep up to date on relevant technologies.

Put the three together, and you have a recipe for defense counsel malpractice that insurers may become liable for. This may have implications and even potentially disrupt current insurer/counsel relationships.

IV. Cyber Liability Insurance Coverage

(Based on material provided by Elissa Doroff, Esq.)

Cyber insurance coverage varies widely by provider, but coverage considerations should include the following, for both third-party claims and first-party mitigation costs following a technology or cyber event:

- Cyber Technology Errors and Omissions
- Privacy and Security Liability
- Data Breach Response and Crisis Management
- Privacy Regulatory Defense Costs and coverage
- Fines and Penalties assessed
- Business Interruption and Extra Expense coverage
- Data Recovery

Coverage premiums will be highly dependent upon the nature and extent of internal systems and controls of the insured, whether such controls are tested regularly, and many other factors.