

Cybersecurity: Are you protected? The threat to law firms is real.

Cyber threats are a growing issue for law firms of all sizes and can be devastating to organizations that house vast amounts of confidential client data. What can we – as law firm marketers do to support our organizations in a cyber event?

Jaffe Senior Vice President Kathy O'Brien recently published [an article](#) with tips about how to recover from a cyber breach. She broke down a hypothetical scenario affecting a law firm to show how to react in the event of a breach. This was incredibly timely since news broke last week that [Foley & Lardner LLP](#) had just faced a cyber event. In this instance, the firm spokesperson was able to quickly confirm that [data was not breached](#) because security safeguards were in place.

Then, in national news, Cathay Pacific Airways [reported a breach](#) of personal information affecting the airline's 9.4 million customers. It has been said that the breach was detected in March and confirmed in early May, but only recently disclosed. Now, the company is warning customers about phishing scams that often follow these types of breaches. Cybersecurity experts are calling for Hong Kong to introduce legislation that would force companies to declare data breaches within days of occurrence.

In other cyber-related news, Girls Scout of America is reacting to a [possible data breach](#) affecting thousands of its members in California. British Airways [says its breach](#) was larger than originally anticipated, and Yahoo has [agreed to pay up to \\$85 million](#) to settle a consumer class action brought about by its recent data breaches. These examples from the weekly news roundup are reminders that data breaches have an impact on everyone – from the very largest companies to small businesses and nonprofits.

Cyber security continues to be top-of-mind for the legal industry. On October 17, 2018, the [American Bar Association weighed in](#), offering guidance (Formal Opinion 483) on ethical duties and best practices after data breaches. The opinion emphasizes the duty of lawyers to notify clients of data breaches, and the importance of law firms having a plan in place to address data breaches before they occur.

"As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach," states the opinion. *"The decision whether to adopt a plan, the content of any plan[,] and actions taken to train and prepare for implementation of the plan should be made before a lawyer is swept up in an actual breach.*

"Even lawyers who take reasonable precautions may suffer a data breach. When they do, they have a duty to notify clients of the data breach ... in sufficient detail to keep clients reasonably informed and with an explanation to the extent



Lisa Altman

Senior Vice President
Public Relations
301.943.9948
laltman@jaffepr.com

necessary to permit the client to make informed decisions regarding the representation."

In Part One of her two-part series, Jaffe CEO/Owner Vivian Hood lays out [how breaches are affecting law firms](#); *the proactive steps to take, and the responsibility that law firms and lawyers must accept to help prevent cyber weaknesses.*

From recent breaches, we have also learned that *how* a firm communicates about a cyber breach is a critical component to managing the impact and mitigating the potential damage to a firm's reputation. Ideally, every organization should have a [crisis communications plan](#) in place in the event of a data breach. It is inevitable that breaches will happen, and marketing and public relations professionals [need to be prepared](#).

Feel free to reach out to me, [Lisa Altman](#), at laltman@jaffepr.com to get your plan in motion.