Navigating Client Notification in the Aftermath of a Cyber-Attack: A DLA Piper Case Study

William Sampson and Jennifer Varon
Shook, Hardy & Bacon

I. Introduction

Law firms are a tantalizing target for cyber criminals. Law firm databases are vaults of valuable information -- intellectual property, business plans and merger strategies, banking information, and other confidential data. Almost weekly, reports of another cyber-attack hit the news. In the first month of 2018, ransomware attacks were reported by six cities, four hospitals or physicians' offices, four corporations, a public school district, and even a county library.[1] In a 2017 ethics opinion, the American Bar Association encouraged attorneys to think of "hacking and data loss in terms of 'when,' and not 'if.'" *See* ABA Formal Op. 17-477.

Though law firms have worked hard to avoid being next in the ever-growing list of victims, sometimes even the best-laid plans go awry. When the worst happens, a law firm must navigate the sometimes murky waters of ethical guidelines, outside-counsel guidelines, and best practices to determine when to provide notice, and how to do it.

Firms who have survived -- and thrived -- in the wake of a cyber-attack can be excellent models for us. One of the most widely-publicized law firm cyber-attacks occurred on June 27, 2017, when a Ukranian ransomware virus related to the infamous Petya virus infected DLA Piper. The attack began at DLA Piper's office in Madrid and quickly spread across the firm's European, Middle Eastern, and American offices. The virus snarled the firm's phone and e-mail systems. After DLA Piper's advanced warning system detected suspicious activity, the firm chose to shut

[1] Kayla Elliott, *Ransomware Attacks of 2018*, TECH TALK (January 23, 2018), https://techtalk.pcpitstop.com/2018/01/23/ransomware-attacks-of-2018/.

down all computers as a precaution. Employees attempting to access DLA Piper's internal web portal were greeted with the following message:[2]

Attorneys and staff remained locked out of their computers for days. Unable to access office phones or e-mail addresses, they were forced to communicate with each other, clients, and opposing counsel using only personal e-mail addresses and cell phones. But clients were not left uninformed. DLA Piper released three public statements in the two weeks following the attack, the third a warm, and adroit, thank you to clients, businesses partners, colleagues, and friends.[3]

---

[2] Staci Zaretsky, *Global Biglaw Firm 'Paralyzed' By New Ransomware Attack*, ABOVE THE LAW (June 27, 2017, 11:14 AM), https://abovethelaw.com/2017/06/global-biglaw-firm-paralyzed-by-new-ransomware-attack/?rf=1.

[3] DLA PIPER NEWSROOM, https://www.dlapiper.com/en/us/news/ (last visited April 3, 3018).

28 JUN 2017

Following reports of a malware attack, a DLA Piper spokesperson said: "On June 27, 2017, our advanced-warning system detected suspicious activity on our network, which, based on our investigation to date, appears to be related to the global cyber event known as "Petya". Our IT team acted quickly to prevent the spread of the suspected malware and to protect our systems.

"We immediately began our investigation and remediation efforts, working closely with leading external forensic experts and relevant authorities, including the FBI and UK National Crime Agency. We are working to bring our systems safely back online."

This statement is an update of a version originally released on 27 June 2017.

3 JUL 2017

Following the widely reported malware incident that occurred on Tuesday 27 June, we have brought our email safely back online, and continue to bring other systems online in a secure manner.

The firm took immediate steps to contain the threat, and we have seen no evidence that client data was taken or that there was a breach of confidentiality of that data.

Our investigation is ongoing and, as always, protecting client information remains a critical priority for the firm.

A note of gratitude to our clients and people

Updated 10 July, 2017

As we begin a new business week, we want to thank our clients and other business partners for the extraordinary support, patience and understanding you have shown us following the unprecedented cyberattack that occurred 27 June. We are proud of the collaborative way our lawyers and staff have all come together, not to mention the support of our industry peers, which has been nothing short of inspiring. Throughout this challenging situation, our people have continued to deliver for our clients with the swiftness, professionalism and determination that is our signature as a firm.

As we have reported, we have brought our email and other tools central to client services safely back online, and are now bringing other major systems online in a secure manner as well.

At all times, protection of client data has been, and will always be, our primary concern. As we also earlier reported, as soon as we became aware of the threat, we took immediate steps to contain the situation. We continue to see no evidence that client data was taken or that there was a breach of the confidentiality of that data.

Thank you again for your understanding and support.

In addition to public statements, sources indicate relationship partners were sent talking points to their personal e-mail addresses or phones that could be used to invite in-depth conversations with their clients. Ultimately, DLA Piper was able to recover its systems and confirm "with a very high degree of certainty" that client data was not compromised.[4] While future law firms falling victim to ransomware may not enjoy such a positive outcome, future victims can certainly learn from DLA Piper's example and structure their breach notification plan in a similar way.

[4] Debra Cassens Weiss, *DLA Piper had planned a cyberbreach response before major malware attack in June*, ABA JOURNAL (December 19, 2017, 4:04 PM), http://www.abajournal.com/news/article/dla_piper_had_planned_for_a_cyberbreach_before_major_malware_attack_last_su.

II. Notification Required by the Ethical Rules

Though the ethical rules do not speak specifically to notification requirements in the event of a cyber-attack, they do provide guidance regarding a lawyer's ethical duty of communication. Model Rule 1.4(a), in part, requires attorneys to:

1) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

2) keep the client reasonably informed about the status of the matter; and

3) promptly comply with reasonable requests for information.

A cyber-attack implicates all three areas. Because the DLA Piper attack prevented attorneys from accessing their firm e-mail addresses, phones, and computers and required them to use alternative means to accomplish client objectives, a notification obligation was triggered under the first category.

The second category "requires that a lawyer give clients advance notice of likely developments that may significantly affect the lawyer's ability to continue the representation." ABA Formal Op. 96-399. Because the massive interruption in service significantly impacted the DLA Piper lawyers' abilities to continue their representation, and dramatically so in the short term, notification was required here, as well.

The DLA Piper hack was widely reported, both in technical and legal journals and in national news organizations such as the New York Times.[5] Even if notification had not been triggered by other portions of Model Rule 1.4(a), it would have been required for clients who learned of the attack and contacted the firm to find out what happened and what it meant to them.

[5] Nicole Perlroth, Mark Scott, and Sheera Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. TIMES, June 27, 2017, *available at* https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

DLA Piper lawyers were almost certainly flooded with client communications seeking information about the attack, their data, and the firm's representation. Even in the event of such a massive influx of requests for information, "[t]he duty under Rule 1.4(a) to comply with a client's reasonable requests for information will obligate legal services lawyers to attempt to respond as well as they can. Although this may temporarily increase the work load of the lawyers, that inconvenience is not an adequate basis for failing to notify clients." ABA Formal Op. 96-399. In such a circumstance, attorneys may "temporarily assign the duty of returning client telephone calls to nonlawyers, who can explain the situation to callers and thus reduce the lawyers' burden." *Id.* But there is little doubt this became an all-hands-on-deck evolution for the entire firm.

The American Bar Association, in a formal ethics opinion, noted Model Rule 1.4(b) is applicable in the case of a breach resulting in the disclosure of confidential client information. ABA Formal Op. 95-398. Model Rule 1.4(b) requires an attorney to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." This means that an attorney must "disclose [the] breach to the client or clients whose information has been revealed . . . [when the] unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter." *Id.*

Further, Model Rule 1.4(b) addresses an attorney's notice obligation when there is a possibility the lawyer has "made a significant error or omission." N.Y. Eth. Op. 734 (Nov. 1, 2000). Whether an error or omission is significant enough to require disclosure under Model Rule 1.4(b) depends upon "the nature of the lawyer's possible error or omission, whether it is possible to correct it . . . , the extent of the harm resulting . . . , and the likelihood that the lawyer's conduct would be deemed unreasonable and therefore give rise to a colorable malpractice claim." *Id.* In

the case of DLA Piper, the cyber-attack did not result in the disclosure of any client's confidential information. But future victims of cyber-attacks may not be so fortunate.

Lawyers are naturally hesitant to reveal information that reflects poorly upon themselves or their law firm. While it may seem easier to avoid communicating adverse information, the failure to disclose errors can run afoul of Model Rule 8.4(c). *See* ABA Informal Op. 86-1518. Further, the comments to Model Rule 1.4 prohibit a lawyer from withholding information to "serve the lawyer's own interest or convenience."

Additionally, the failure of an attorney to disclose his own malpractice to a client may result in civil liability for the lawyer or his law firm. *See Olds v. Donnelly*, 696 A.2d 633, 643 (1997) ("The Rules of Professional Conduct still require an attorney to notify the client that he or she may have a legal-malpractice claim even if notification is against the attorney's own interest."); ABA Formal Op. 08-453; *but see Fitch v. McDermott, Will & Emery, LLP*, 929 N.E.2d 1167, 1184 (2010) ("We similarly find no case that would require an attorney to affirmatively advise his client of his negligence and the statute of limitations for suing him.").

The ethical rules additionally provide guidance on when notification must be provided. The comments to Model Rule 1.4 require "prompt" notification, when feasible. In the midst of a devastating cyber-attack, immediate notification may not be possible. And hasty notification may cause additional problems if incorrect information is communicated in the rush to get a message out. The comments to Rule 1.4 suggest a law firm may be better served by using a tiered notification approach: initially communicating only basic information, indicating when a more detailed response may be expected, and then following up with details as they are available.

DLA Piper took this tiered notification approach in its public communications after its attack. Its first statement, included above, said an attack had occurred, an investigation was

ongoing, and the firm was working to bring the systems back online. This short statement achieved the goal of providing notification about known facts of the attack but avoided the temptation to release too much information in the early stages. Nearly a week later, the firm could say there was "no evidence that client data was taken or that there was a breach of confidentiality of that data." Future victims of cyber-attacks should consider DLA Piper's multi-tiered notification approach as a way to ensure "prompt" notification pursuant to Model Rule 1.4, without running the risk of providing misleading information, in violation of Model Rule 8.4(c).

III. The Impact of Outside Counsel Guidelines on Breach Notification

Many clients distribute guidelines to their attorneys that set out the policies and procedures the client expects the law firm to follow during their relationship. Mindful of the business imperative behind them, attorneys may accept the proposed outside counsel guidelines verbatim, without negotiation. Once accepted, the guidelines become the governing document of the relationship, overriding the engagement letter and imposing contractual obligations on outside counsel. Many of these guidelines set specific requirements in the event of a suspected data breach or cyber-attack.

The Association of Corporate Counsel (the "ACC") developed Model Information Protection and Security Controls for Outside Counsel Processing Company Confidential Information ("Model Controls") to assist in-house counsel in establishing procedures for their outside counsel to protect the company's confidential information.[6] The Model Controls provide suggested security protocols and breach-response measures and address many aspects of client

[6] ASSOC. of CORP. COUNSEL, Model Information Protection and Security Controls for Outside Counsel Processing Company Confidential Information (2017), *available at* http://www.acc.com/advocacy/upload/Model-Information-Protection-and-Security-Controls-for-Outside-Counsel-Jan2017.pdf?_ga=2.18008698.2105555974.1496154508-4598426.1496154508.

confidential information. Specific to data breaches, the Model Controls require outside counsel to notify in-house counsel of any "suspected or actual unauthorized disclosure, loss, or theft of Company Confidential Information" within 24 hours. After the initial notification, the Model Controls require law firms to provide timely updates and to respond to any requests for information. The law firm is asked to designate one knowledgeable individual who is available 24/7 to respond to client inquiries. In addition to notification requirements, the Model Controls require outside counsel to identify a root cause of the breach and provide remediation.

While it is impossible to know what outside counsel guidelines DLA Piper had agreed to, it appears the firm's response tracked the ACC. An initial communication was made within 24 hours of DLA Piper's awareness of the cyber-attack. Additional information was released as it was available. Relationship partners were sent additional talking points and were available for their clients' inquiries. DLA Piper determined the root cause of the cyber-attack. And the breach was resolved without any evidence client data was compromised.

Relationship partners should reacquaint themselves with the outside counsel guidelines for their clients. While the guidelines may include provisions similar to the models discussed above, they may also include different, more stringent requirements. Each relationship partner should have sufficient familiarity with her own client's guidelines that an appropriate, prompt response can be made to a breach. Relationship partners should have printed copies of outside counsel guidelines available in case a cyber-attack prevents them from accessing their electronic files, which is a distinct possibility.

Law firms should also take care to review outside counsel guidelines before they are signed. Many contain indemnification provisions that, if invoked in the event of a data breach,

could either overwhelm, or invalidate, liability coverage. These provisions may be negotiable. Even if they are not, an awareness of the provisions up front prevents surprises down the road.

IV. Notification Best Practices

While the ethical rules and outside counsel guidelines provide the outer limits of acceptable notification, a cyber-attack forces additional considerations not explicitly covered there. The best time to work through these considerations, of course, is before the breach occurs. While there is no one-size-fits-all solution, the notification element of the firm's response plan might do well to include the following:

- **A template initial notification containing basic information about the cyber-attack and the law firm's response.**

  Law firms may wish to model this initial notification on DLA Piper's June 28, 2017 communication. Drafting template notifications in advance allows for a better final product as drafters can work on getting the communication right rather than starting from scratch. A template notification almost assures faster notification when an attack does occur.

- **A notification chain of command.**

  The response plan should clearly lay out who has authority for the message, who will work on the notification team, and how the ultimate message will be distributed to each client. The plan should include alternative methods of contacting each team member in the event law firm phone and e-mail addresses are disabled. Law firms should include back-up team members in case an original team member is unavailable or unreachable after the attack.

- **A record keeping mechanism.**

The response plan should allow the law firm to document what notification reached each client and when. This is important in the chaos following a cyber-attack. And in the event of a later ethical or legal challenge, notification records will be crucial to establishing proper procedures were followed.

- **Planned table-top notification exercises.**

  These exercises allow law firms to run through their breach response plans in advance, ensuring everyone is prepared and revealing problems with the plan.

- **A list of outside vendors.**

  Outside vendors can be critical in the hours following a cyber-attack. A vendor can set up and provide support for a 24-hour hotline, allowing clients to contact the law firm with questions at any time. A similar service can be set up using e-mail.

- **Keep hard copies handy.**

  Law firms should have a hard copy of all aspects of the cyber-attack response plan in case the attack renders electronic systems unusable, as it did at DLA Piper. Formatting the cyber-attack response plan as an easy-to-follow checklist, with action items and their owners identified, would also be helpful.

Running parallel with the requirements found in the ethical rules and the outside counsel guidelines, a law firm's paramount consideration is to provide the appropriate, prompt response in a manner that best preserves their relationships with their clients. Even if a client's outside counsel guidelines do not require notification until 72 hours after a cyber-attack, a law firm should consider providing it sooner. Clients keen to learn of any potential loss of their data or the interruption in their legal services will want to know about it immediately, even if <u>they</u> were responsible for the 3-day notice period!

V. Conclusion

"A cyber-attack can ruin your whole day!" But, with proper planning, law firms can minimize their impact and their duration. An understanding of the notification required by the ethical rules, outside counsel guidelines, and best practices allows law firms to respond promptly and effectively.