The 2017 DLA Piper Breach Revisited

by Sharon D. Nelson, Esq. and John W. Simek

It was more than a year ago that the 3,600-lawyer global megafirm DLA Piper was brought to its knees by a data breach in June of 2017. One of the questions we hear most often when we lecture is, "If DLA Piper can be breached, how do the rest of us stand a chance of preventing a data breach?"

It's a valid question. The reaction last year varied with the size of the law firm. Larger law firms focused a lot on purchasing or increasing their cyberinsurance coverage after the DLA Piper story made the headlines. They also amped up their security measures, and pried open their wallets to create stronger defense-in-depth strategies.

The smaller firms also began spending more money on cybersecurity, many of them now awakened to the dangers of a breach. From our foxhole, small to mid-size firms particularly began to focus on employee cybersecurity awareness training, newly aware that their greatest asset (their employees) is also their greatest risk. Since 2017, cybersecurity awareness training has been the CLE that we have most often been asked to present.

Employee training is extraordinarily helpful since phishing emails present one of the greatest dangers to law firms – and these emails are becoming increasingly sophisticated as the bad guys hire native English-speakers to help craft the emails. They also do more research and even perform advanced reconnaissance. As an example, they may know that the managing partners "Andrew Jones" or "Jillian Smith" sign their emails as "Andy" or "Jill." Much information is publicly available via law firm sites, social media sites or press releases. We make it easy to devise inviting phishing emails.

It is hard to imagine how horrified DLA Piper's lawyers must have been when the attack came. A sign greeting DLA Piper's Washington employees on June 27, 2017 said, "ATTENTION DLA EMPLOYEES – All network services are down. Do NOT turn on your computers. Please remove all laptops from docking stations & keep turned off. *No exceptions.*" Not the usual greeting when you come to work, is it?

The cyber attack took down the firm's phone systems and most of its computer networks, though some systems were shut down as a preventative measure. Two weeks after the attack, the firm issued a statement indicating that some systems were still being restored.

In a world in which large law firms are mostly paperless, the managing partner of DLA's D.C. and Northern Virginia offices indicated that the firm had re-established the old practice of having paper copies of phone numbers and other necessary information needed to keep the firm functioning in the event of another cyber crisis. That manager, Jeff Lehrer, said that the firm has made a lot of improvements to its infrastructure.

He also indicated that the original attack was against the Ukraine, where DLA Piper has an office. The person who presumably clicked on something malicious did so because of an update to accounting software unique to the Ukraine (and needed for tax filings). That person was an administrator with administrative privileges which aided in the spread of the attack.

The malware, which falsely presented as ransomware at the outset of the attack, was later identified as "NotPetya" which destroys data, though presumably DLA Piper had good backups in place as it reported that no data was lost.

All in all, we talk to audiences about DLA Piper's measured handling of a dramatic event. Two public statements were issued, but there was otherwise not a lot of reliable information and even the press was loathe to speculate overmuch. Things were much quieter than we imagined possible. It appeared to us that the law firm's management did a pretty good job of handling a very difficult situation.

At the end of 2017, DLA even beat its own budget numbers, in spite of losing significant billable time. Hard to argue with that kind of good news – DLA Piper certainly demonstrated resilience. Was there something wrong with DLA's cyber defenses? Undoubtedly, though no specifics were made public. And we imagine considerable time and money have been invested in remediating the specific problems uncovered and looking for and then remediating other security issues. As a side note, we still don't understand why the email systems were down for so long and why email messages were not being delivered. Senders were getting rejection messages for sent email. Even if you host your own email servers, you should have technology in place to spool delivery and/or provide cloud access to your mailboxes should your physical server fail.

But whatever the weaknesses in DLA Piper's defenses, it survived the crisis bloodied but still standing tall at year's end. Other law firms watching had to be hoping that they could do as well.

The authors are the President and Vice President at Sensei Enterprises, Inc., a digital forensics, cybersecurity and legal technology firm based in Fairfax, VA. 703-359-0700 (phone) sensei@senseient.com, https://www.senseient.com.