LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cybersecurity & Privacy Group Of The Year: Crowell & Moring

By **James Boyle**

Law360 (February 1, 2024, 4:10 PM EST) -- Helping Microsoft stop the source of disruptive cyberattacks, advising large corporations on recovering from a Russian-linked ransomware attack and providing guidance for major military contractors on stronger U.S. Department of Defense regulatory standards earned Crowell & Moring LLP a spot on Law360's 2023 Cybersecurity Practice Groups of the Year.

Launched about 10 years ago, Crowell & Moring's privacy and cybersecurity group has evolved into one of the top practices in the country, advising major corporations on the types of technology issues that have come to affect any business with a networked computer. The firm counts among its clients Microsoft, Honeywell, Huntington Ingalls Industries and DXC Technology.

Practice co-founders Evan Wolff and Jeff Poston recently told Law360 one of the main contributors to the group's success is the combining of privacy and cybersecurity in one practice. Both are interconnected, they said, and keeping them separate would only slow the group's progress.

"The worst thing we could have done is silo those two groups off," Poston said. "Our objective is to gain a broader understanding of what works and what doesn't through the integrated group, and I don't think we are being immodest when we say we have accomplished that."

Poston and Wolff manage the privacy and cybersecurity practice from the firm's Washington, D.C., office. Started in 2013, the group has grown to more than two dozen attorneys in nine U.S. and international offices, including Chicago, Los Angeles, New York, San Francisco, Brussels and London.

The growth continued into the new year as Crowell & Moring announced in January the additions of Linda Malek, Jason Johnson and Blaze Waleski to the privacy and cybersecurity practice in the New York office. The trio moved their practices from Moses Singer LLP and have also joined Crowell & Moring's healthcare practice.

"This is a priority growth area for the firm," Wolff said. "We've been given the full support of the executive committee. We have a strategic approach to our growth, and have recruited laterals and built internally. We collaborate to focus on speaking with clients with one voice, which has contributed to the success of the practice."

Privacy and cybersecurity concerns are not confined by state borders or expertise areas, and

communication between the national and international offices is crucial, Poston said.

"What we have built is a global practice," Poston said. "This can become an overused cliché, but culture matters. The culture of this firm is premised on collaboration. Client issues are interrelated, and we have attorneys with different backgrounds that can address them. People like Evan are steeped in technology, and others like me come from more of a litigation background. Our communication helps us become more integrated."

The combination of technology savvy and litigation expertise translated into Crowell & Moring's successful shutdown of major sources of ransomware attacks against Microsoft and the company's clients. For years a number of Microsoft clients had endured attacks by several hackers, including two Russian-speaking gangs, which tricked users into downloading malicious software.

Microsoft tasked Wolff and Poston's team to find a way to halt the attacks, and in March the group won a temporary restraining order and multiple rounds of preliminary injunctions in New York federal court by arguing the hackers violated Microsoft's copyright and trademarks. With the restraining order, Microsoft was able to seize malicious domain names and uncover and block nearly 2,000 nefarious IP addresses.

"A lot of our time is spent on pure incident response, when data and systems are at risk," Poston said. "What we're usually doing is defending a client from an attack. With the Microsoft case, we were able to go on offense and go after the bad guys."

Crowell & Moring's cybersecurity team was back on defense in May, when several companies turned to the practice for help in the wake of a ransomware attack on file transfer platform MOVEit Transfer. The group worked to assess how the hacker group gained access to the program, determine how the clients could comply with notification standards and map out potential next steps.

The growing threat of sophisticated cyberattacks has led the U.S. Department of Defense to adopt stricter guidelines for third-party contracts. Contractors were notified in 2021 they would need to achieve cybersecurity maturity model certification by this fall to retain their contracts.

The exact details of the new rules were released late last year, and Crowell & Moring's cybersecurity practice members were able to quickly interpret the language, send out alerts to their clients and host several webinars on the changes and immediately counseled dozens of companies.

"Really what differentiates us is our deep technology know-how — starting with Evan and [partner] Matt Welling," Poston said. "It is such an advantage when you are in the trenches with a client. For most lawyers, when the IT folks are talking, there is a massive language barrier. But at the end of the day, you need to talk to the general counsel and to the chief information security officer, and they don't have time for a learning curve in the midst of a crisis."

--Additional reporting by Tracy Read. Editing by Linda Voorhis.
