Credit: Illustrations by Andrew Lyons

Peeling back the mask

Vincent Manancourt | **03 October 2019**

Traditionally, hacking victims wanting to retaliate have had little choice but to rely on law enforcement. Now, a growing band of them are increasingly turning to the US court system – and the extensive discovery powers it endows – to take matters into their own hands.

In late 2017 and early 2018, several members of Republican party fundraiser and venture capitalist Elliott Broidy's entourage, including his wife, received Gmail security alerts asking for their usernames and passwords, which they apparently provided.

Shortly thereafter, media reports containing the Broidy's private emails began appearing across the US.

As it turned out, Broidy had been the victim of a cyberattack. After obtaining usernames and passwords, hackers gained access to a trove of his company's documents and correspondence, including trade secrets and business plans.

The hackers then packaged the information into documents, which they sent to journalists across the US. Forensics reports done at the time strongly indicated that the attack was perpetrated by Qatar – a nation Broidy had publicly lobbied against. For its part, Qatar denies any involvement.

For Daron Hartvigsen, a managing director at Ankura, the cyber investigations company that worked on the case, the intention of the attack – to smear rather than make money – indicated that a nation state rather than a criminal group may be behind it.

"If you're hacking into a system with criminal motivations the intended effects might be to harvest credit card information, PII or those kinds of things, whereas with a nation state the intended effects are maybe different … in some cases they could be to harvest data that would achieve some strategic goal," he says.

An example of a strategic goal, he says, is to use the data gleaned to discredit a target and "reduce that person's ability to influence the political spectrum".

As a hacking victim, Broidy is not alone. Verizon says that 30% of phishing emails are opened by those targeted, while according to anti-hacking software provider Retruster, there has been 65% growth in the number of phishing attacks in the past year. Nation states, drawn by the ability to attack at a low cost, have developed a particular taste for hacking, including phishing.

Traditionally, the response to getting hacked has been twofold: focus inward by securing data, handling compliance obligations and assessing the damage; and, depending on the damage, call in law enforcement.

But a new approach, spearheaded by lawyers and other data specialists who have, for the most part, spent time in government is taking root in the US: suing through the civil courts.

And that's just what Broidy's legal team did.

Lee Wolosky, a Boies Schiller Flexner partner who has held national security positions under three US presidents, led that team. Speaking generally, he says there are two main benefits of turning to civil litigation after being hacked: "money and control".

"When you turn over your evidence to a law enforcement agency, you don't control the investigation, you don't control the output, you don't control public disclosure. You don't control anything," he says.

But an affirmative line of attack, he says, allows you to “control everything”.

“You control how the investigation is conducted, you may be able to control disclosure of it to the public. And you are seeking damages, which in many cases can be millions and millions of dollars.”

Miller & Chevalier partner Kirby Behre, who also has experience of using this approach and is representing a hacking victim against a UAE investment fund, puts it this way: “If you want to get compensated for what has been done, then you’ve got to go to civil court. If you try and prosecute someone criminally who’s out of the US, good luck trying to get a prosecutor interested, but even if you do it’s not going to result in anything monetary.”

Working with a prosecutor is a “one-way street” in terms of information flow, he says: “They put you in a black box and you don’t know what they’re doing … they don’t tell you if they’re doing a lot of work, a little work, they could drag their feet and nothing could be done for months and months and months, while the evidence disappears.”

Indeed, Cooley partner Travis LeBlanc, who also represented Broidy, says that even if you notify law enforcement, they don’t even have to investigate, and will do things at their own pace.

“It’s going to take them quite a while to get the various search warrants issued … it could be that years down the road there is a prosecution but the vast majority of these cases do not result in prosecution,” LeBlanc adds. “The government doesn’t have to determine who was behind this and necessarily it’s going to exercise prosecutorial discretion to decide when it should investigate and invest resources in something.”

He adds that relying on law enforcement doesn’t just mean surrendering control, but also giving them access to your systems. “You have to go through a calculus of whether you want to invite law enforcement in to actually have full access to your network and then once they have the investigation, it’s largely in their control,” he says.

From public to private

“It’s so often that for most companies when they are the victim of a cyber incident the knee-jerk assumption that is made is that they were at fault, that they had poor security practices,” says LeBlanc. “But in many circumstances there is just a well-resourced bad actor who exploited an otherwise secure environment.”These are not the only benefits to using civil litigation to pursue hackers, proponents say. Hacking victims are often on the wrong side of publicity. Using civil litigation, a victim of an attack can begin to paint a clearer picture of what has happened, and perhaps go some way towards shifting the narrative.

This is particularly true of nation state backed attacks: if a party with those kind of resources is going to devote its attention towards trying to break into a network, it’ll probably succeed eventually, notes LeBlanc.

Hartvigsen makes the point that the story that civil litigation helps reveal may lead people to reconsider what it means to be a victim of a cyberattack and who is held accountable.

But damages can be an elusive goal.

First, in most cases it is a challenge knowing whom to sue. In the Broidy case, there was enough forensics evidence pointing to Qatar for it to be sued directly, but often it is too difficult to tell. In those cases, lawyers use John Doe actions to build on forensics evidence using subpoenas, which allow them to extract information from companies that hackers have used to carry out the attack.

Wolosky describes the approach this way: “In the US where lawyers have subpoena power, it is possible to use the tools that private lawyers have to compel the production of documents and electronic records in a manner that enables you to unravel even very complicated hacking schemes that use obfuscation techniques to try to hide their origins.”

He says the approach is not particularly new, just a marrying of “new technological challenges with old legal techniques”.

> Many of those pursuing the civil litigation approach have served in public office. Boies Schiller partner Lee Wolosky doesn’t think that’s a coincidence. “Some hacking activity is undertaken for commercial reasons, some of it is undertaken for political reasons. I think those of us who served inside of government have a deeper appreciation of the overall context in which much of this activity is occurring and that’s helpful for us in going out and litigating cases as private citizens,” he says.
>
> Wolosky himself joined Boies Schiller in 2001 from the White House, where he served as director for transnational threats on the National Security Council under Presidents Bill Clinton and George W Bush. From 2015 to 2017, Wolosky served as President Barack Obama’s special envoy for Guantanamo.
>
> Before joining Ankura, Daron Hartvigsen held several roles within the US Air Force Office of Special Investigations. In early December 2017, his unit’s partnership with the Department of Justice, the Pittsburgh Federal Bureau of Investigation field office and the Naval Criminal Investigative Service resulted in the indictment of three Chinese nationals for theft of US intellectual property.
>
> Between 2014 and 2017, Travis LeBlanc served as the enforcement bureau chief at the Federal Communications Commission, having formerly been special assistant attorney general of California and senior adviser to the state’s then Attorney General – and current presidential candidate nominee – Kamala Harris. He also previously served in the Obama Administration in the US Department of Justice’s Office of Legal Counsel, which advises the President, Attorney General and general counsels of executive branch agencies.

A John Doe action is a key part of lawyers’ arsenal since, hand in hand with data forensics, it allows them to build up information in an iterative process. The actions can be useful even if they don’t uncover the source of an attack in enough detail to identify a named defendant: getting hold of email account information or IP addresses, for instance, can allow plaintiffs to protect themselves against further attacks from the same source.

Even if you can name the defendant, however, the route to damages can be rocky. Sometimes they just won't turn up, and the default judgment you get in these cases is difficult to enforce. Lawyers who specialise in going after sovereign states often warn clients that they may never be able to recover damages they win in court.

And if the defendant does turn up, nation states in particular will fight aggressively to get the lawsuit dismissed – usually on foreign sovereign immunity grounds, as Qatar was able to do against Broidy (though he is appealing).

Passed in 1976, the Foreign Sovereign Immunities Act (FSIA), generally prevents nation states from being sued in US court, with some exceptions. The sturdiest of these is the commercial activities exception, which allows cases against nation states to continue if plaintiffs can prove that the case in question is sufficiently linked to "commercial activity" by the state in the US or that has effects in the US.

Broidy's team tried and failed to trigger this exception. But a case in Washington, DC, federal court has given them cause for hope. Early last year, UAE investment arm Rakia failed to get a hacking lawsuit against it kicked out on sovereign immunity grounds.

In that case, US–Iranian businessman Farhad Azima's lawyers – which included Miller & Chevalier's Behre – were able to convince the court that alleged hacking of his email and subsequent blackmailing were linked to US commercial activity.

"Azima has plausibly alleged that Rakia's engagement in certain commercial activity – using Azima as a mediator and partnering with him in foreign business ventures – caused Rakia to commit the hacking for the purpose of influencing the ongoing mediation, punishing Azima if anything went wrong with those negotiations, and ultimately 'gain[ing] leverage and coercive influence' over Azima," the court said at the time.

The court also noted Azima's allegation that he was threatened by Rakia that he would become "collateral damage" in the "all-out war" that Rakia planned to wage against its former chief executive (Rakia had called on Azima to mediate a dispute with the ex-chief executive). The case was ultimately dismissed on appeal.

While Azima overcoming sovereign immunity has encouraged those championing the civil litigation approach, Behre strikes a cautious note: "If you are pursuing the government itself then it will be a more difficult task."

Indeed, for those who represented Broidy, the case has revealed the FSIA's incompatibility with the modern world.

"We have got to keep in mind that FSIA was not written for a world in which we had computers and electronic devices that would allow a foreign government on one side of the world to attack a private individual or company on the other side of the world without ever setting foot on the land of the nation state where the victim is located," LeBlanc says. "It may be that we are at a point where it is worth considering amending the act."

Hartvigsen says it simply: "Things like that are just out of date."

Wolosky says that change is likely to come from Congress, rather than the courts, since judges have "generally declined to create an exception through the judicial process".

Nevertheless, the judiciary may see the need for an update. Indeed, in throwing out Broidy's case against Qatar, the judge overseeing the dispute wrote: "Given … the growing prevalence of attacks in cyberspace, it may be an appropriate time for Congress to consider a cyberattack exception to the FSIA, which at the moment effectively precludes civil suits in US courts against foreign governments or entities acting on their behalf in the cyberworld."

For now, even if litigation ultimately does not end in damages, Wolosky says, it is still a path worth pursuing. "If you are able to unmask a group, you can alter their conduct and thereby serve a broader public purpose." Showing a willingness to pursue litigation can

also act as a deterrent to future hackers. As one lawyer puts it, “Bullies tend to pick on the weakest.”

Broidy’s case against Qatar ended up revealing the identity of over 1,000 individuals who had been targeted by the same hackers. “We uncovered 1,200 other victims in this case. We’re talking about foreign heads of state; we’re talking about heads of intelligence agencies; we’re talking about royalty; we’re talking about ambassadors from several countries,” Leblanc says.

Those people now have proof that they have been targeted by hackers and can take steps to protect themselves, he says. “We could only achieve that kind of transparency through subpoena power.”