COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 11. November 05, 2020 From Her Words to OCR's Ears: 'Dissent' Seeks to Hold Hackers, Leakers Accountable

By Theresa Defino

In her 14-plus years of investigating and blogging about hacking and breaches, "Dissent" has been yelled at, threatened with lawsuits and accused of being a criminal. But now the self-described "older than dirt" retired New York psychologist, who publishes her work at DataBreaches.net, is enjoying a bit of fame.

Recently the HHS Office for Civil Rights (OCR) gave Dissent props for warning Athens Orthopedic Clinic PC in 2016 that patient information was online and for sale, an incident that predicated a $1.5 million financial penalty.[1] It wouldn't be entirely accurate to say that, up until now, Dissent has been toiling in obscurity, but OCR's mention prompted *RPP* to learn more about her and the insights she's gleaned over the past 26,000 posts on DataBreaches.net and 19,000 on her other website, PogoWasRight.org.

In a wide-ranging Q&A, Dissent was by turns funny, self-effacing and humble, saying her work is simply "the right thing to do if you care about privacy," and repeatedly claimed: "I am not a security professional." A " bad businesswoman" who doesn't make money from the blog (she does do some consulting), Dissent is unsparing in her criticism of organizations' dumb mistakes that let hackers in and is impatient with those who ignore her when she tries to notify them that their information is "leaking all over the internet."

Much of the blog consists of timely postings of stories by others, but Dissent will often provide commentary—some undoubtedly unique given her psychology background and time spent talking to hackers, which few can claim. She also does a fair amount of original reporting, making the site a must-read for busy HIPAA compliance professionals.

Although never the victim of a HIPAA-related breach herself, Dissent's interest grew from being harassed and stalked online and was spurred by a desire to share with others what she had learned about staying safe online. In 2006, Dissent launched PogoWasRight.org to report privacy news. Although it gets its name from the cartoon character who said, "We have met the enemy, and he is us," it is not affiliated with the comic strip (which ended in 1975). She launched DataBreaches.net in 2009.

Unfortunately for Athens Orthopedic, the reason the world knows about Dissent's tip is that the organization, according to OCR, had numerous HIPAA violations underlying the hack. Athens was just one in a trio of settlements totaling $10.65 million that had the common theme of "you were warned" (the FBI raised the alarm in other cases).

Despite Athens' containment efforts—which Dissent termed slow and somewhat misguided—the hacker group The Dark Overlord, after stealing credentials from Quest Diagnostics, rummaged around the practice's network for six weeks, according to OCR.

In the first part of the interview, Dissent discusses more about the Athens case and what she has learned about the mind of a hacker. In the second part, to be published in the December issue of *RPP*, she describes how companies react when she contacts them and offers suggestions for controlling the damage from breaches.

RPP: **The first thing people might want to know is why you don't use your real name.**

D: I'm pseudonymous because I still have people that I irritate the hell out of who try and harass me, stalk me and defame me. I used to worry that maybe the criminals that I was reporting on might seek revenge, but I'm not quite as worried about that anymore. The criminals are actually better in some respects than the noncriminals when it comes to stalking and harassment. But I'm not going to let people who are evil or who are obsessed stalkers or whatever get me to the point where I cannot share information that I want people to have. I also choose to be pseudonymous to keep the privacy blogging part of my life separate from my professional work as a psychologist.

RPP: **Has OCR ever mentioned you in a settlement before, and what was your reaction to seeing that?**

D: This is the first that I know of. I've seen my name show up in other things, in federal court cases. Prosecutors and the government may list reporting I've done as part of the evidence presented against criminals. I'm surprised that OCR would mention anybody. But I do know they read my blog and the complaints I file.

I don't remember if I complained to OCR about Athens. The whole time I was reporting on Athens, I kept complaining about them in my postings, noticing what's going on, that patient data was being dumped…Why aren't they getting it removed? Why am I having to get it removed? There were all kinds of things that Athens Orthopedic didn't do well. They had more than a dozen clinics at that point, I think. And yet they publicly stated they had no insurance to offer patients credit monitoring.

RPP: **Were you satisfied with a two-year corrective action plan (CAP) and $1.5 million penalty to which Athens agreed?**

D: Yes. In addition to the hack, what I also think is important is to look at the other things the entity did not do well. How do you not have business associate agreements in place? Quest was hacked. That's how The Dark Overlord got the credentials and logins. But when did Quest notify Athens that Quest had been hacked? Did they notify them in May? In April? Or was it after June 14 when Athens was hacked? Because if Quest notified them promptly, that's even more curious and means they probably never changed the passwords.

RPP**: Do you think CAPs, in general, improve security and privacy when they are implemented**?

D: I think they would be better if they were implemented sooner. I think waiting three or four years—when things may have already changed—is a shame. But I think HHS has done a really good job over the last few years of making the point that you have to do a risk assessment. You have to know what assets you have, you have to know where they are, and to do this annually. You have to have a plan in place.

RPP: **Do you suspect being mentioned by OCR will bring more views to your page?**

D: People read my little site and use it. But most people don't know about it because Google will not consider me a news site; they will not index me under news since I'm not using my real name. I don't check statistics or analytics on my page. I'm probably not doing this blogging thing right. I finally got on LinkedIn about a month ago. I'm still trying to sort that out. I'm not a very good business woman. My site is still noncommercial. I ignore all the requests about sponsored posts but would welcome overall sponsorship.

RPP**: Had you previously heard back from OCR about a breach?**

D: Yes. There was a group of doctors who are actually not far from me. A researcher found patient data of theirs exposed on a non-HIPAA-compliant server. He had a lot of trouble contacting them, and he contacted me. I didn't get anywhere either. They didn't respond to notifications. So I called the chief privacy compliance officer

for the health system the doctors were affiliated with, and she reached out to the doctors and got them to lock down the data. Then I filed a complaint with OCR, because it shouldn't have been that hard to notify them or get them to respond, and they were using a non-HIPAA-compliant server.

OCR got back to me after a year to say they had worked with the medical practice and shared all the changes the medical practice has now made to be compliant. In other cases, I've gotten calls from OCR if they needed clarification or wanted to know if I had proof of some point. In a few cases, I've seen where all of a sudden the numbers the entity reported on the OCR breach portal have been changed to numbers that are more in line with what I showed OCR. I even apologized to one OCR employee about sending them so much and was told they actually value it. But they don't investigate everything I send them. I have sent them some really big, messy cases, and they have sidestepped them. They may just not have the resources to do it all.

RPP: **Let's discuss The Dark Overlord and hackers. In September, Nathan Wyatt pleaded guilty to being part of The Dark Overlord, which hacked Athens, and was sentenced to five years in prison and a fine of more than $1.4 million.[2] Did you ever speak to him?**

D: Not over the phone, but I chatted with him and others in The Dark Overlord. Nathan was affiliated with The Dark Overlord in its early days, and his screen name was "Crafty Cockney." He had other aliases. I chatted on Jabber with Nathan numerous times beginning in September 2016 and even after his arrest. He opened The Dark Overlord's Twitter accounts, phone accounts, email accounts, bank accounts, and PayPal account. He also claimed he had mentored "the kid" who he called "Dark"—the original spokesperson who tweeted and wrote their extortion emails and press releases. The original spokesperson claimed to be the leader of The Dark Overlord.

RPP: **What are hackers' motivations? Can they be stopped?**

D: There are different motivations. There were people in The Dark Overlord who had a lot of anger and obsessional issues. And if the hacking victim didn't respond the way the original spokesperson thought they should or had to respond, they would get intensely emotional and angry and escalate the threats. It was all about power and control. There were things they were doing at that point that were absolutely horrific. They locked down a Montana school district for a month. They were sending messages to the parents' phones saying they were going to kill their kids. They bragged to me that they were going to try and get a kid to commit suicide and speculated about what a gay student would do if they outed him. It's unfortunate that more were not caught. I hope law enforcement does figure out who they are.

So you have kids who want money, but they also have control-emotional issues. Then you have those who are strictly money-oriented, like some of the current crop of ransomware coders and operators. They've got your data, and you need to figure out how to deal with them or negotiate with them. There are companies and law firms out there that have built a reputation for dealing with ransomware and hacks. And maybe they can get them down 20% in their demands. Ransomware demands have increased astronomically this past year.

Then you have the kids who are on a whole different level, and a lot of them are almost addicted to hacking. If we could take these young people and redirect them that would be great. This is when I take off the journalist hat and I'm more like a mom-psychologist. But there are a number of kids who have turned their lives around, and I'm always thrilled when a kid I chatted with and tried to redirect manages to change course and become a white hat. I am really so proud of them.

RPP: **Are hackers super-sophisticated or are entities making basic mistakes?**

D: Some of the hacks are not sophisticated at all. Entities will leave the remote desktop protocol enabled when

they don't need it on. There's a way in. Entities are not patching right away when there's a vulnerability. If you don't patch within one day, somebody's going to be exploiting it. So there are things that entities are doing wrong. And I'm not a security professional, but it seems to me that there are some things that we've known about for a long time, and they're still a problem. And you have to go, "Why?" Is it just mom-and-pop businesses that don't have enough support? But then you have a big hospital system that just got attacked. And if they don't have the means to protect themselves successfully, who does?

Phishing, email and social engineering are still big ways in. And how do you stop those? Are you going to stop having employees respond to email? You can keep training on how to recognize phishing, but you only need to slip up once and it's all over.

***RPP*: Why do you say you are not a security professional?**

D: I could not hack my way in or out of a paper bag if my life depended on it. If you held a gun to my head and said, "Do an SQL injection," I don't even know how to pronounce it much less do it. But I read and I learn. I ask questions of some very smart people who generously share their knowledge with me.

Contact Dissent at breaches@databreaches.net.

1 Theresa Defino, "Settlement Involves 'Dark Overlord' Hack, Tip by Breach-Tracking Journalist," *Report on Patient Privacy* 20, no. 10 (October 2020), https://bit.ly/3dYqpd5.
2 Department of Justice, "UK National Sentenced to Prison for Role in 'The Dark Overlord' Hacking Group," news release, September 21, 2020, https://bit.ly/34PR1dC.