

Ethical hackers: Thinking like criminals but wearing the white hats.

by Gail Appleson, Communications Editor,
Armstrong Teasdale LLP

When it comes to protecting clients from security breaches, lawyers generally provide advice on such key matters as policies and compliance. But Armstrong Teasdale attorneys Dan Nelson and Lucas Amodio have added a new twist to their legal services. They've learned how to hack into computers and have even earned a credential to prove it.

These two lawyers became "Certified Ethical Hackers" during 2014 through the International Council of E-Commerce Consultants (EC-Council). An "ethical hacker" is an information security professional trained to penetrate networks and/or computer systems using the same methods and techniques as a criminal. But ethical hackers, also called white hat hackers, use their skills to assess and improve security by finding vulnerabilities. And unlike criminal hackers, they have permission to break into computers from the organizations who hire them.

There are more than 700 EC-Council accredited training centers across 107 countries. The training program is offered locally by Hacker University™, a subsidiary of the St. Peters, Missouri-based ethical hacking firm, Parameter Security.

"On the privacy side, we (lawyers) can have meaningful conversations with our



Nelson

Amodio

clients about their duties to retain and protect information," said Nelson, an Armstrong Teasdale litigation partner and co-chair of the firm's Data Security and Privacy Practice Group. "But on the security side, what do lawyers really know about how to protect them? Lawyers and IT people don't have a good history of communicating. How do we bridge that gap?"

A commercial litigator with some 22 years of trial experience, Nelson advises

clients about policy and procedures aimed at protecting data. To enhance his practice, Nelson became a Certified Information Privacy Professional. This major credential, issued by the International Association of Privacy Professionals, indicates that a holder knows U.S. data protection laws, key privacy terminology, and practical concepts concerning the protection of personal data and trans-border data flows.

Despite this extensive legal background, Nelson felt he needed more extensive computer skills if he was truly going to help clients in this age of constant cyberattacks. As a result, he pursued the ethical hacking credential.

Amodio comes from the other side of the equation. An intellectual property lawyer who focuses on high-technology and computer-related matters involving patent law, Amodio is former software engineer who obviously knows the IT talk. But for him, the ethical hacking course was a way to better assist his patent clients. For example, one of his clients is a credit card company and the course has helped him better describe several security-based patents.

"I've been a computer geek all of my life," said Amodio who started programming games when he was only seven-years-old. "I've done plenty on my own computer to get past stuff, but I never learned about hacking. So when Dan started talking about the program I thought it looked cool."

The ethical hacking course does require a high level of computer proficiency, so it's not for all lawyers. In fact, Parameter officials said Nelson and Amodio are the only two attorneys that have successfully completed the local program.

Although Amodio was already familiar with many of the terms, Nelson, who describes himself as being a "tekkie nerd at heart," put in about 250 hours of study before even taking the course.

"If you don't have a technical background, then you will have to invest

the time to get one," he said.

The program, which costs \$2,250 per person, is five intensive days of work. As part of the course, students learn to think like attackers, understanding their motives and strategies. They also acquire skills aimed at recognizing and analyzing the latest security threats; identifying security breaches and determining acceptable risk within organization.

"Learning how to hack is kind of a dangerous tool to have," said Amodio. "It's incredibly easy to do if you have the time and patience."

Amodio explained that students are expected to be able to

The ethical hacking course does require a high level of computer proficiency, so it's not for all lawyers.

break into a computer in a lab setting, however, they also must sign an agreement that they will never hack without written permission.

At the end of the course there is a four hour exam, which both Nelson and Amodio described as being extremely tough.

"I was probably more worried about passing this test than the bar exam," Nelson said. "I don't see a flock of lawyers doing this," added Amodio.

But for those who have the ability and determination to take on the challenge, helping clients obtain security is the reward.

"People perceive the most fundamental problem in cybersecurity to be only an IT problem, but it's not," said Nelson. "It's a problem that starts with lawyers and centers around compliance and the management of people. If we can bridge the gap between IT and in-house lawyers, we've added a lot of value. When you can make that conversation happen, that's really when you start talking about being secure." ■