CyberInsecurity News™
WHAT LAWYERS NEED TO KNOW

MAY 2019

HOW ONE LAW SCHOOL DECIDED TO TACKLE CYBERSECURITY

After lots of planning, the public launch was an annual conference.

BY DAVID HECHLER

Lawyers and technology may not be a natural match, but the days when attorneys could think of themselves as above all that are long gone. And no one knows this better than the deans at law schools.

Law school deans are always looking ahead for the challenges their graduates will soon be encountering. That's part of the job of preparing tomorrow's lawyers. And Robert Wilcox, dean of the University of South Carolina School of Law, saw cybersecurity as an area he couldn't ignore.

"You're always looking to be sure that you don't fall behind and miss a curve that's beginning to form," Wilcox said. "And this looked like a wave. So we felt like we needed to get on board."

The school now has lots of plans in the works. "What we would like to have ultimately is a certificate program or maybe even a master's program in cybersecurity that would be aimed at lawyers for post-JD work or at [chief information security officers] and [chief information officers] who might benefit from having a legal understanding to go along with their technological understanding," Wilcox said.

But they're not just planning for the future. "We're encouraging the faculty to make technology more broadly a part of every course we teach at the law school," Wilcox added. "Law students have to be conscious, whatever field they're going into, of how cybersecurity will affect their ability to be hired by clients." (For more on Wilcox's planning, see the sidebar below.)

PHOTOGRAPHY BY CARISSA MCKINNEY

The First Conference

In April, the school held what amounted to a coming out party: its first annual conference on this subject. Billed as the Cybersecurity Legal Institute, it packed a lot of information into one very full day.

The subjects it covered included: ransomware, cyber insurance, business email compromise, artificial intelligence, third-party vendor risks and the California Consumer Privacy Act (full disclosure: I moderated the panel on this topic).

There were also speeches by representatives from two government agencies that play leading roles in this area. Maneesha Mithal, associate director of the Federal Trade Commission's Division of Privacy and Identity Theft, reviewed some of the 60 enforcement actions the FTC has pursued to date (but not the ongoing discussions with Facebook). She also explained

UNIVERSITY OF SOUTH CAROLINA
School of Law

the policy work her organization undertakes, much of it involving education and advocacy that leads to studies, recommendations and testimony before Congress.

The other speaker was Daniel Sutherland, chief counsel of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. Sutherland talked about CISA's responsibilities and the emerging threats it's working to address. Three big ones, he said, are supply chain risk, election security and the conflict between law and technology. (CyberInsecurity News will feature a Q&A with Sutherland in the coming weeks.)

Among the breakout sessions, the panel on artificial intelligence was particularly interesting. One speaker discussed how it's being used by law firms and the other talked about how in-house lawyers can use it.

Artificial Intelligence Is Already Here

Andrew Arruda is co-founder and CEO of ROSS Intelligence. He's also a lawyer, and he talked about the various ways AI can perform tasks that save lawyers from hours of tedium. You can train a system to do legal research. If you tell it what you want, and what you don't, the program can go though the case law and tell you the relevant cases to read and which ones are on point.

Arruda quickly addressed a common anxiety. There are no robot lawyers, he said. Robots can replace associate gut work. But we still need lawyers to take the results and run with them.

Lawyers will not be replaced by machines any more than bank tellers were replace by ATMs. There are more tellers now than there were before the advent of ATMs, he said. And right now, he added, only 20 percent of Americans who need legal services can afford them. AI may help cut the costs.

It's just another way of delivering legal services, he added. "It will lead to, in my opinion, more jobs in law." But they won't look exactly the same. "AI is not going to replace lawyers," he concluded. "Attorneys who use AI will replace those who do not."

Ryan Benjamin, an attorney at Microsoft, described a host of programs that can save an in-house lawyer time and improve efficiency. They can speed work with contracts and patent applications, and they can save a fortune on document reviews.

There are legal chatbots—like virtual assistants—that can perform small tasks, while other programs can answer basic legal questions. Instead of spending 30 minutes tracking down information, you spend 30 seconds, Benjamin said.

When he's out of the office at a conference (such as the one he was speaking at), Benjamin can set up a program to answer common questions that colleagues ask so that they don't have to wait until he returns, and he won't face a blizzard of requests when he does.

The Truth About Cyber Insurance

What would a cybersecurity conference be without talk about data breaches? During the cyber insurance panel, Andrea DeField, an associate at Hunton Andrews Kurth, had some statistics handy. Her firm has covered 1800 breaches so far. She has read that the average amount a company spends to recover from a breach is $7 million.

The session was filled with warnings, as might be expected given the topic. Joe DePaul, head of FINEX cyber/E&O, North America, said the subject is overrun with misinformation. Many articles on cyber insurance talk about policies that were not actually cyber policies, he noted.

Abigail Oliver, assistant VP of cyber underwriting at AXIS Capital, talked about how quickly expenses can mount after a breach. Forensics alone can be very expensive. PR bills can add up. Then there's legal advice, lost income, business interruption.

It's all part of the equation when companies think about cyber insurance. "It's something everyone needs to consider right now," said DeField.

There was another point on which they all agreed: Consult with your lawyer early and often. At every step of the way. This includes when you're considering what coverage you need, applying for insurance, reviewing the terms (breaches are sometimes called "cyber terrorism," DeField said, and you want to be sure this language is covered). And, of course, you want to work with your lawyers when you're filing claims.

Other tips? DeField pointed out that many policies don't cover breaches where an employee's personal device was involved. Companies are wise to make sure that there isn't a BYOD exclusion. And DePaul noted that if a company is hit with a ransomware demand, it's going to need a Bitcoin wallet if it decides to pay the ransom.

He asked for a show of hands of everyone whose company has a Bitcoin wallet. No hands went up.

Tabletop Set with Humor

The day's final session was a tabletop exercise—or rather a talk about how one works—led by three cyber specialists from Kroll. At the end of a long day, the advice was useful. But so was the packaging. The information was leavened with humor, and it always drew laughs.

Isaiah Jensen said that successful hackers sometimes have a problem selling the stolen data. It isn't always easy finding a buyer and effecting a transaction. That's the beauty of ransomware, he said. "They've actually found the perfect person to sell your data to. Turns out the perfect person is you!"

Keith Novack reviewed the protocols you want to follow after a cyberattack is detected. The incident response plan must be accessible and clear. Everyone on the team must be contacted quickly. And third- party partners must also be contacted. Arrangements with them should always be set in advance, Novack emphasized. "Googling 'forensics' during an attack is not the way to go."

One of the most important points, Jensen underscored, is having an offline backup that's easily accessible. And the

UNIVERSITY OF SOUTH CAROLINA School of Law

key decisions are who will declare an incident, when it will be declared and whether to pull the plug on the network. This should be a business decision, he said, not an IT decision.

In explaining why, Jensen cited a large financial institution that learned it was losing lots of money that was being siphoned out of its network. IT was asking whether to pull the plug. But before they could be given an answer, someone had to calculate how much they were losing compared to how much they would lose by shutting down the system. Who makes that call should be set in advance, Jensen said. And it's best if the executives are involved at that point, so the lines of authority are clear.

At the end of the day, some gaps are almost always uncovered during a tabletop exercise, said Greg Michaels. Part of the point of doing them, he noted, is to find the gaps and work to correct them.

And while they were talking about lessons learned, Jensen lightened the mood one more time. "The best time to do lessons learned is after a tabletop exercise," he said. "The second best time is after an actual attack."

HOW THE UNIVERSITY OF SOUTH CAROLINA SCHOOL OF LAW PUT TOGETHER A CYBERSECURITY CONFERENCE: AN INTERVIEW WITH DEAN ROBERT WILCOX

CyberInsecurity News: *When did you start thinking about hosting a conference?*
Robert Wilcox: The conference was put together this year in about six or seven months. About a year ago we were thinking that we needed to do it, but it takes a while to get the people in place to plan it. The serious planning began in the fall. We're about to begin the planning for next year's conference, so we'll have a little more lead time.

CIN: *What were your hopes for the inaugural conference?*
RW: My main hope was to put together a group of speakers that would be viewed as knowledgeable experts at a national level—folks who would bring in the expertise of government and the corporate world in this area. I was hoping for a conference that would reach those more familiar with cybersecurity while not being too complex for those who are just becoming aware of it. If there was a single hope, it was to increase the awareness of the importance of this subject—that it is not something, particularly in the legal field, that can be ignored.

CIN: *How did you go about putting it together?*
RW: It was primarily by putting together the task force that we drew upon—particularly people that [task force co-chair] Karen Randall knew to bring in from around the country. And then we used that group, with their wide range of knowledge and expertise, to identify what were the most important issues today and who the best people to come in and speak about them would be.

CIN: *Karen Randall chairs the cybersecurity and privacy practice at Connell Foley LLP. How did her involvement begin?*
RW: Karen is an alumna of the law school who came down to speak. In addition to our courses, we have a technology program about every two weeks. Many of the topics are cybersecurity-related, and Karen had come down to visit the law school and to speak at a class. It was the perfect opportunity—a moment when I was looking for somebody who would help us put together a cybersecurity program.

CIN: *We're speaking 11 days after the conference. How do you think it went?*
RW: I was pleased with it. I have learned a few lessons about some things to do differently—in terms of efforts to involve the audience more proactively. But my impression was the conference fulfilled my goal of making sure that people understand that this is not a subject that you can hide from and hope it will go away. And I think they got a lot of their questions answered about some of the big issues.

CIN: *Are there any big-ticket items that you know you want to change or introduce for 2020?*
RW: I don't know at this point that I have any specific ideas for what the program will look like. One of the things I've learned about this area in my short time being involved in it is the landscape can change very quickly. And I want it to develop into the conference that you go to if you want to know the latest of what's happening. I don't want it to be last year's news. I think we have to be careful to always have room for some hot topics fit into the program fairly late in the process.

CIN: *Do you have any sense of whether your law students are particularly energized by cybersecurity and privacy?*
RW: The honest answer is there is a small group that is very energized by it—they are very, very interested. There is a slightly larger group that is conscious of the concerns, and they're very interested in being on the cutting edge of it. I think there's still a group—students and faculty—who have not yet fully become aware of how pervasive the subject is going to be in their careers.