IADC COMMITTEE NEWSLETTER

CYBER SECURITY, DATA PRIVACY AND TECHNOLOGY

August 2017

IN THIS ISSUE

With the recent WannaCry cyber attack, the discourse among cyber security escorts about threat actors has increased in intensity but tends to be one-dimensional. The underground hacker conference Def Con 25 challenges conventional thinking about hackers and provides a transparent and insightful look into hackers' motivation and methods.

Def Con Hacker Conference: An Accidental Tourist's Observations

ABOUT THE AUTHOR

Elizabeth S. Fitch is a founding member of Righi Fitch Law Group. She is a trial attorney with over 30 years of civil defense experience and has the AV Preeminent Rating. Beth has defended numerous multi-million dollar cases ranging from catastrophic injuries to construction defect cases. She has represented all types of professionals from lawyers to architects. Because of her defense of insureds under general liability insurance policies, Beth has successfully handled the entire gamut of complex tort cases ranging from construction mishaps to products liability. In 2016 she was again recognized as a Super Lawyer and is a sustaining member of Arizona's Finest Lawyers.

Beth is certified by the International Association of Privacy Professionals. The CIPP/US certification is the preeminent privacy credential in the US private sector. Beth is the Co-Chair of the Arizona State Bar's Cyber Liability Committee and serves as the Co-Dean of the CLM School of Cyber Claims. She counsels companies and insureds on cyber hygiene and best practices and responding to data breaches and advises clients on privacy and cyber security involving PII, PHI, and PCI, serves as a breach coach and leads the firms data response team. She can be reached at beth@righilaw.com.

ABOUT THE COMMITTEE

Corporations and law firms around the world are constantly dealing with cybersecurity, data privacy and other important technology issues, both in business and, where available, in litigation discovery. Burgeoning technologies are placing new and increasing demands on in house and outside lawyers and their clients. All are being challenged to meet new and strict data privacy and security guidelines and the consequences for failing to meet these requirements can be devastating. The Cyber Security, Data Privacy and Technology Committee will address the differing substantive laws globally in these areas, and be of interest to many other committees whose members and activities are impacted by technology. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Elizabeth S. Fitch
Vice Chair of Publications
Righi Fitch Law Group
beth@righilaw.com

DefCon is an annual event in Las Vegas that draws over 15,000 hackers from all over the world to show off their latest cyber exploits. Def Con organizers claim that it is the world's longest running and largest underground hacking conference. Def Con attracts hackers, IT security professionals, government agents and one accidental tourist…me. Having now practiced law in the cyber security space for six years, I have attended or spoke at more than a dozen cyber security conferences, all of which have been informative and well organized but none that focused on threat actors. Since I wanted to better understand cyber hacker motivation and methods, I decided to attend Def Con 25.

Def Con 25 blew my mind. From beginning to end, this conference was like no other. Def Con 101 is a seminar for "newbs" (Def con's definition for first timers) which I dutifully attended since I was a newb. When the second speaker stood up and yelled into the microphone "Welcome Bitches! We are here to f%@* with you", I knew I was in for a wild ride. And wild it was. From the hacking tournaments to the vendor booths where the latest and greatest hacking tools were being sold, the entire thrust of the conference was about exploiting cyber vulnerabilities.

The hacking community was also unique and extraordinary. The organizers at Def Con 101 set the expectations and ground rules. Never have I ever been at a conference where the attendees are given such explicit instructions. First, there is the 3-2-1 rule: Three hours of sleep, two meals, and one shower. Evidently experience has shown that these enthusiastic hackers are so into what they are doing that they literally forget to sleep, eat, and shower. Second, the "don't be a dick" rule: everyone at the conference is smart and passionate and therefore on equal par so don't be arrogant and presumptuous and most importantly don't try to show off by embarrassing a speaker. Third, don't be stupid: this is a hacking conference so don't use the public network. Finally, the organizers gave impassioned talks about engaging and pushing oneself out of his/her comfort zone. Toward that end, the Def Con 101 seminar wraps up with a "kegger". Engagement turned out to be quite easy…even for an old accidental tourist like me. Whether standing in line for the next presentation, observing hacking contests, or just hanging out in the "Chillout" lounge, everyone is friendly and wants to talk everything cyber. I was a bit of a novelty being one of the few privacy attorneys in attendance so curiosity about what I do drove many of the conversations, but I learned quickly that asking for a business card or offering to exchange information was a conversation buzz kill. Indeed, conference attendee's identities were carefully guarded by the conference organizers. Registration is on a cash basis only. While blank name tags are handed out, there is no place to put your actual name. Instead, the name tags provide a space to write in your "alias".

The most unique aspect of the conference is the "villages". These are designated rooms where hackers gather to either compete or learn how to break through industry specific technological security measures. At the "Internet of Things Village", hackers participated in contests to hack off-the-shelf smart devices. Similarly, the goal of the "Car Hacking Village" was to teach village goers about that latest smart car hacking techniques and tools. Def Con's voting booth village was the big hit and widely publicized in the national news. Suffice to say, the hackers took less than 90 minutes to exploit weak and outdated security measures to gain full access.

The social engineering village was the most fascinating. I watched hackers successfully use scams to collect confidential information from unsuspecting company employees. Here's what happens: A designated hacker is placed in a sound proof room as the audience watches her use OSINT information collected earlier to manipulate individuals over the phone to reveal "flags" of information. One hacker successfully obtained a company's Federal Express number in a 30 second conversation. Another hacker convinced an employee to participate in an innocuous survey that was then used to drive the employee to a fake website and download malicious code.

Unbeknownst to me, I was staying at the venue for the "Black Hat" conference. This conference is closely related to Def Con in that both were founded by the same ingenious hacker and entrepreneur. Unlike Def Con, Black Hat draws mostly a professional crowd. The differences between the two conferences could not have been more stark. While I will probably attend Black Hat next year because the focus is on helping companies mitigate cyber threats, Def Con gave me a whole new perspective on the imminent cyber threats that are on the very near horizon. My biggest takeaway: absolutely nothing connected to the internet is safe and Def Con is the undisputed evidentiary predicate for the trite saying in cyber security circles that "a cyber breach is not a matter of if but when." With that said, I now have new found appreciation for the hacker community that has been demonized and think that harnessing the passion and talent of hackers can improve not only cyber security but also quality of life. The Def Con founders welcome letter says it all: "One thing I am certain of though is that hackers will help point the way through this jungle of self-serving marketing speak, technically impossible tech policy, and insecure products to give the public a real view of what is possible and what isn't. It won't be the organized crime groups, vulnerable companies, or governments doing this, but instead hackers through a deep understanding of technology that can speak truth to power."

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

MAY 2017
Doe v. Backpage.com and its Aftermath: Continued Uncertainty and New Litigation in the Wake of the Supreme Court's Denial of Certiorari
David Patrón

APRIL 2017
Incorporating Technology into the Management of the Work Processes at the Firm
Donna L. Burden, Elizabeth S. Fitch and Park L. Priest

FEBRUARY 2017
"The First Thing We Do, Let's Kill All The Lawyers"
Elizabeth S. Fitch and Elizabeth Haecker Ryan

DECEMBER 2016
A Primer for Understanding Blockchain
Doug Vaughn and Anna Outzen

AUGUST 2016
The Attorney-Client Relationship in the Electronic Age
Elizabeth S. Fitch and Theodore M. Schaer

MAY 2016
Understanding the Defend Trade Secrets Act of 2016: "We're Not in State Court Anymore"
Peter J. Pizzi and Christopher J. Borchert

DECEMBER 2015
Cyber Armageddon: Survival or Annihilation?
Theodore M. Schaer and Elizabeth S. Fitch

JULY 2015
Fitbit Data Brings Another Dimension to Evidence
John G. Browning

DECEMBER 2014
The Ethics of Technology in E-Discovery – An Introduction
Peter J. Pizzi and Julia L. Brickell

SEPTEMBER 2013
Emerging Technology and Its Impact on Automotive Litigation
John G. Browning

JUNE 2012
iPad Apps: Brave New Frontier
Adam Bloomberg and J. Calhoun Watson