Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Connecting The FBI's Cyber Agents With Its Brick Agents

By **Richard Frankel**

Law360, New York (July 14, 2017, 1:19 PM EDT) --

Richard Frankel

When I joined the Federal Bureau of Investigation in 1995, it was the beginning of a new era at the agency. My class of special agents-in-training received the same instruction in the law, investigative techniques, defense tactics, physical fitness and firearms use, taught to hundreds of other classes that preceded us. But what was different was that we were a part of the introduction of information technology tools, electronic communications practices and cybercrime capabilities that has come to redefine the agency over the last several decades. Today, the FBI is the lead federal agency for investigating cyber activities by criminals, overseas adversaries and terrorists.

These were the early days of a new breed of agent called the "cyber agent." The cyber agent chased criminals in cyberspace from a screen, in an agency dominated by "brick agents," who chased criminals on the streets. We were the first class to be trained to use the FBI's new computer system to write reports and memos that would be connected throughout the FBI's 56 field offices and headquarter locations. Of course, today the FBI is connected by wire, Wi-Fi, smartphone and other technologies on numerous networks and with several levels of classifications.

Making Cyber Agents Better Communicators

Threats to cybersecurity have increasingly become more common, more sophisticated and more dangerous and they affect individuals, business, government, and institutions. Consequently, when the FBI hires special agents today, it is not simply looking for lawyers and accountants. Among the highest-priority hires today are applicants with backgrounds in cyber-related professions or college majors. Almost every case the FBI now handles involves some type of cyber or information technology or tools (smartphones and/or the internet not to mention more sophisticated technology used for intrusions, phishing schemes distributed denial-of-service attacks and so on).

The FBI also wants its new special agents to have been successful in prior careers. In fact, joining the FBI as a special agent is, and always has been, a second career for new hires, who join the agency with real world experience. One of the key skillsets the FBI expects new special agents to have is interpersonal communications skills so they are effective communicators. In my own case, the basic investigative skills that I learned early in my career were vitally important in my role at the FBI, which included increasing interaction and cooperation between law enforcement and the greater intelligence community to identify and combat cyber threats.

These communications skills are critical to effectively interview victims of crimes, engage effectively with witnesses who may have information on counterterrorism, interrogate criminal suspects or try to convince someone involved in a national security investigation to become a source for the FBI. But as the agency added more special agents with cyber experience, it found that those new agents, while they are subject matter experts in cyber matters and cyber-based communications, are not as skilled in vital interpersonal communication.

Compounding this issue is the explosion of cybercrimes and threats, where the FBI does not have the necessary amount of specially trained cyber experts on board. Subsequently, when the cyber special agent has been identified, he or she many times is sent directly to specialized squads to begin their work, where they don't receive the needed on-the-job training and guidance from the experienced agents in dealing with people. Ideally, the FBI would partner the experienced "old dogs" with the "new pups" to show them how to operate with the public, teach them arrest skills when appropriate, and how the FBI special agents carry themselves when dealing with the public.

Veteran FBI Agents Learning Cyber Skills

Because FBI agents generally retire in their 50s with 20 or more years of service, most will seek a third career, often in security or a related field. However, to be more competitive in the job market, these investigators, who may have spent decades going after mobsters, fraudsters or national security targets, need to have competence in cyber-related investigations. Ironically, they are in a similar position to the new cyber agents, who may lack some of the communications and investigative "street smarts" that the seasoned agents have.

Recently, I spoke with an agent who had been on a gang/violent crime squad most of his career and had become a supervisor in that area. He was looking at the next phase of his career after the FBI and realized that not many jobs outside of law enforcement existed where investigating gangs and "kicking in doors" were prerequisites. Therefore, when he was offered a spot on a cyber squad, even though technically the job was considered a demotion, he took it. For a while, he wondered if he had made the right choice, given that he was at least 10 years older than the others, and found himself sitting behind a desk.

But then something happened: One of the newer cyber agents was discussing how to get information from a witness and the experienced brick agent offered his expertise and guidance. The brick agent gave them the instructions, went with them on the "operation," provided advice when needed, and established a rapport with the target of the interview. After a conversation with the witness was started and the need to get technical information from the person was identified, the agents switched leads and switched roles. This back-and-forth continued until the case came to a successful resolution with a target being arrested. The veteran agent told me that because of the success that he experienced in this new squad, he recruited several of his old gang squad partners to join the cyber squads. By dealing with new agents who have great skills for investigating cyber matters, veterans learn how to investigate cyber intrusions, DDoS attacks, ransomware, mirroring of hard drives, etc.

A lot changed at the FBI in the 22 years that I served, before moving on to join a private law firm. Cybercrimes and threats — especially counterterrorism, counterintelligence and internet crimes — have become serious threats to our institutions, our citizens and our nation. The tradition of seasoned veterans guiding new agents through ad hoc on-the-job training to give them the skills to operate more effectively and efficiently on the street is probably as old as the FBI, but needed as much as ever. But, so

is the need to train older agents in the skills that can combat cybercrime while at the agency and in their next career.

Richard Frankel is of counsel at Ruskin Moscou Faltischek PC in Uniondale, New York, and co-chairs the firm's cybersecurity and data privacy practice group. He previously led several FBI field divisions as the special agent in charge. He also served as the associate director of national intelligence and senior FBI representative to the Office of the Director of National Intelligence.