NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

TECH b•e•a•t

From Summer 2009 *TechBeat*

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Exercising CyberSecurity

Security at a major defense contractor has been breached. Information points to an insider with access to advanced technological information. Quickly, a team consisting of company staff, law enforcement and local government assembles to determine the best way to handle the situation.

Fortunately, the above situation happened only in a tabletop exercise: Intrusion Forensic Experiment 2 (IFX 2), held in September 2008 in Rome, N.Y., and designed by the National Law Enforcement and Corrections Technology Center (NLECTC)-Northeast. The exercise's 19 participants visited virtual offices and labs, collected evidence, listened to video statements and collaborated on a theory of responsibility. When the exercise ended, a post-analysis session helped participants understand the method and motive behind the attack and the actual computer forensic findings. In addition to developing closer working relationships with each other, participants took information on how to create their own tabletop exercises back to their agencies.

The Northeast Center, a program of the Office of Justice Programs' National Institute of Justice, used lessons learned from IFX 1, held in June 2007, to build on and create IFX 2. Developed at the request of the Upstate New York Electronic Crime Coalition, IFX 1 focused on an incident at a financial institution. Both tabletop exercises were scalable in size, scope and location, all of which would help an agency develop its own exercise.

In IFX 1, developers created a fictitious credit union, including employees, a Web site, a network diagram and information technology policies and procedures such as an incident response plan, acceptable network usage policy and an operations manual. IFX 1, a heavily scripted exercise, had strategically placed decisions for each participant; in IFX 2, the scenario took on a more free-flowing form.

The primary objectives of IFX 2 included raising the awareness level of the participants regarding insider threats, developing and strengthening relationships with and among law enforcement agencies, emphasizing the importance of indications and warnings in identifying cybersecurity issues and stressing the importance of defense in depth and total enterprise/agency security. IFX 2 also had secondary objectives of increasing awareness related to malware capabilities, technology exploitation, insider threats, security countermeasures and the need for strong audits and awareness programs. Participants and observers came from the Air Force Research Laboratory/Information Directorate, the FBI, the U.S. Secret Service, and the Utica (N.Y.) Police Department, in addition to private sector and academia representatives.

"The goal for the first exercise was primarily to build relationships between law enforcement, the private sector and government agencies," says Tracy Nitti, IFX project manager. "We wanted to get them in the same room and working together so they would be comfortable if they did have to collaborate on a real case." The majority of the participants in the first exercise belonged to the coalition and its members wanted to build on the groundwork for relationships laid within that group.

"With the second one, we took the success we had with the first exercise and scaled up technically," Nitti says. "By using a different sector for the crime, we were able to introduce an exercise where the motive and means were different." Some of the original participants returned for IFX 2; for others, it marked their first exercise.

"We really enjoyed the interaction we had from a technical/social perspective and the way we were able to determine suspects, method of modus operandi, the motivation behind the criminal enterprise and what the individual's background was," says Agent Tim Kirk, U.S. Secret Service, of his participation in IFX 2. "All those things together really made a great exercise."

"I thought the exercise was an excellent opportunity to not only preplan some of our operations and the way we do business, but also a great opportunity to meet the

other participants," says Sgt. Anthony Martino, a computer forensics specialist with the Utica Police Department.

Both exercises were designed for 15 to 20 participants to keep the group at a manageable size. However, for IFX 2, a separate group of observers did watch the exercise from a second room.

"They became so involved and excited, they wanted to participate too," says the Northeast Center's Debra Cutler. "These vulnerabilities exist pretty much across the board. Every part of the country could experience these types of problems."

For more information or to request a copy of the NLECTC-Northeast developed report titled,* How to Design a Cybersecurity Tabletop Exercise, *contact the Northeast Center at (888) 338-0584.

This article was reprinted from the Summer 2009 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center System, a program of the National Institute of Justice under Cooperative Agreement #2005–MU–CX–K077, awarded by the U.S. Department of Justice.