Microsoft's opens facility to crack down on cybercriminals

November 22 2013, by Janet I. Tu

In a building on the north side of Microsoft Corp.'s Redmond, Wash., campus, there is much talk of stopping the bad guys.

By that, the Microsoft employees do not mean Google Inc., Apple Inc. or Amazon.com Inc.

Rather, the investigators, forensics experts, engineers and lawyers staffing Microsoft's new Cybercrime Center talk about stopping criminals: software pirates, criminal syndicates that run botnets and exploiters of children.

Microsoft opened the doors last week to its multimillion-dollar Cybercrime Center, a 16,800-square-foot facility that is one part crime-fighting headquarters and one part sleek showcase for Microsoft technologies.

Part of the reason Microsoft developed the center was to make sure it had the latest state-of-the-art tools it needed to fight increasingly savvy criminals.

"As the cybercriminals are getting more sophisticated, our abilities are getting more sophisticated," said David Finn, associate general counsel of Microsoft's digital-crimes unit, during a tour of the facility last week.

The center brings together company units that focus on piracy and intellectual property theft, and on digital crimes, including botnets and

malware and technology-facilitated child sexual exploitation.

About 35 of Microsoft's 100 employees worldwide employed in those units are now based in the Cybercrime Center, which also includes Microsoft technologies such as Site Print, which can map online organized-crime networks, and PhotoDNA, which helps find and remove some of the worst images of child porn online.

Large touch screens from Perceptive Pixel, a company Microsoft purchased in 2012, line the walls, showing off Excel Power Map, a 3-D data-visualization tool.

In large workspaces cordoned off behind glass walls that can convert from transparent to opaque, forensics teams look over evidence, while malware teams map online-crime networks.

Down another corridor, a line of offices reveal rooms that can be occupied by visiting crime-fighting partners, such as those from law enforcement or academia.

"We designed the center with partners high in our minds," Finn said.

Another reason Microsoft created the center is to have a place to bring visiting dignitaries and leaders to give them an idea of how various Microsoft technologies could be used - not just for investigating crimes, but also for handling and analyzing large amounts of data for use in businesses and other organizations.

Microsoft already has an Envisioning Center, where it showcases technologies as part of its vision of future workplaces, homes and "third places," such as retail stores and restaurants.

The Cybercrime Center, in contrast, shows off the technologies in

action, "where people are actually working," said Brad Smith, executive vice president and general counsel at Microsoft. "I wanted to create a place where people - government or businesses - could see how we're using our own technology."

Like the Envisioning Center, the Cybercrime Center is not open to the public.

The center does not address the issue of government spying. Microsoft, along with other tech giants, have come under fire for their roles in U.S. national-security surveillance. In response, the companies are fighting in court to be able to disclose more information to the public.

Smith said Thursday that the new center "isn't about spying. It's about fighting crime."

He declined to say how much the center cost, except to say that it was a multimillion-dollar investment. He added that the cost was largely recouped in a recent agreement reached with one of the cybercriminals the center's team had caught.

Microsoft's digital-crimes unit has helped take down or disrupt seven botnets tied to criminal organizations in recent years.

Botnets are networks of virus-infected computers remotely controlled by cybercriminals. A botnet could surreptitiously control an infected device to use, for example, for harvesting personal information, sending out spam messages, taking screenshots or promoting websites that exploit children.

Among those that Microsoft has helped disrupt are the Citadel botnets, which enabled a cybercrime ring to access half a billion dollars after stealing online-banking information and personal identities, and the Nitol

botnet, which could lurk in brand new computers.

The Nitol botnet illustrated how cybercriminals are preloading some PC hardware from unsecured supply chains with infected counterfeit software, according to Microsoft.

It makes sense then, said Zoe Krumm, a Microsoft senior manager of forensics, for the malware and forensics teams at the company to work together even more closely now, as they will be able to in the new center.

"We're starting to see those intersections between malware and forensics more," she said.