



Username	Password
<input type="text"/>	<input type="text"/>
<input type="checkbox"/> Keep me logged in	<input type="button" value="Log In"/>

[Home](#)
[About Us](#)
[PERF in the News](#)
[Announcements](#)
[Publications](#)
[Resources](#)
[Services](#)
[Membership](#)

When individuals fall victim to cybercrime, they often report the offense to their local police department. But most police officers lack the knowledge or tools to respond in a meaningful way. In 2019, the New York City Police Department implemented a pilot program to help its officers respond to the typical cybercrime complaints they receive.

The pilot program was for “cyber-enabled” crimes, as opposed to “cyber-native” crimes. Ravi Satkalmi, Deputy Director for Intelligence Analysis at the NYPD, explained the difference:

“Cyber-enabled crimes are traditional crimes that now have a new mode for delivery. They might be committed online, though social media, or through cell phones, but they’re still traditional crimes.”

For example, cyber-enabled crimes include financial frauds that are carried out with digital technology, identity theft, purchase of illegal drugs online, phishing and pharming scams in which victims are tricked into releasing personal or financial information through fake emails or websites purporting to be legitimate banks or other businesses, and many other types of crime.

“Cyber-native crimes are those that can only be committed because we have these tools. They didn’t necessarily exist as crimes before these tools were available.”

Cyber-native crimes include crimes in which a computer or other digital system is the target of the attack as well as the means of the attack, such as malware attacks, and hacking of government agencies’ or corporate databases.

PERF spoke with five current and former members of the NYPD to learn more about the pilot program and other steps they are taking to address cybercrime.

Announcements

[Click here](#) to view PERF’s April 15th webinar: *Managing Demonstrations: New Strategies for Protecting Protesters and the Police*

[Click here](#) to read past editions of “Trending,” PERF’s weekly email update to its members, including the most recent: [“What If the Police Shared Ownership for Managing Demonstrations with the Community?”](#)

THE CHALLENGE POSED BY CYBERCRIME



Deputy Chief John Hart, Intelligence Bureau

The [recent FBI IC3 report](#) showed a 69% increase in total internet crime complaints from 2019 to 2020. I don’t think that’s just due to COVID; I think there’s also better reporting of these crimes.

However, we're still just scratching the surface of what's out there. And the FBI only has the ability to investigate a very small portion of those complaints. That's not a criticism, it's just a fact.

The DHS Cybersecurity and Infrastructure Security Agency (CISA) is doing a great job helping state and local law enforcement as well. But ultimately we all have to become better at this.

We had done a pilot cybercrime program at the end of 2019. We released the report at the beginning of 2020, but then all our energy and time went into COVID and police reform. I think we learned some important lessons from the pilot, and we want to work with all our partners on how we can better handle these cases.

The FBI looks at two things when deciding whether to take a cybercrime case. One is if it meets a certain dollar threshold. The other is whether it's committed by nation-state actors, rather than local criminals. Those two things separate us and our federal partners in all crime. It's important for us to know where that separation is, what they do, and what we should be doing at a local level.

But I know that patrol cops everywhere are not equipped to handle these crimes. They say, "It's cyber, so I don't know what to do. Let me pass it on to someone in my agency who's a specialist."

THE PILOT PROGRAM



Nick Selby, former Director of Cyber Intelligence and Investigations

When we started the pilot, there was skeptical questioning about whether the patrol cops would be interested. But after training more than 700 patrol officers in New York, I can tell you that they're very frustrated. Many of them have family members who have been victims of scams on their computers and phones, and we see it on the news and hear it from the community outreach workers and the Grand Larceny Division. So they're very aware of these crimes, but they just haven't been given the tools and training to handle them.

And the cyber special agents at the FBI are brilliant, but to ask them to look at a crank phone call where someone lost \$6,000 is like asking Mick Jagger to do the sound check at a Rolling Stones concert. They're very busy with very complex things. So there should be some way to fill the gap below that threshold.

Working with Deputy Chief Hart, Chief Thomas Galati, Deputy Commissioner John Miller, then-Commissioner James O'Neill, and Assistant Commissioner Rebecca Weiner, we saw the problem of cybercrime as one where we just didn't know what the answers were. We didn't know the most common scams, who was getting scammed, or where they were getting scammed. For the NYPD, an agency that measures almost everything, that was unacceptable.

In early 2019, Commissioner O'Neill and Deputy Commissioner Miller gave me the mandate to start looking at this. Because we weren't measuring these crimes, we had to scan our records management system, and look at millions of calls to find the calls that

look like cybercrime. Those cybercrimes are things like fraudulent phone calls, bank account takeovers by someone who fraudulently obtains the password, and phones being taken over through "[SIM swapping](#)." This group of cybercrimes would not include things like ransomware, critical infrastructure attacks, or nation-state attacks.

Over the course of the first six months of 2019, we searched diligently for cases that looked like what we wanted to focus on. Using that information, we estimated that in 2018 there were about \$230 million worth of these kinds of cybercrimes in New York City. That's big, because during that same period, car thefts totaled about \$50 million in New York City.

We presented this information and asked for the resources to do a pilot program. Everyone agreed this was worth trying. We decided to do it in Queens South, because we wanted a place that was busy enough to get significant numbers, but not so busy that we might get in the way of more serious investigations. We got help from the Queens District Attorney's cyber unit, and by the second half of 2019, we were ready to start.

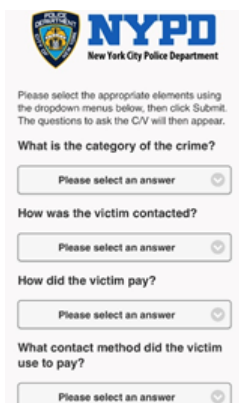
We created a 15-minute training program that educated cops about cyber-enabled crimes. Over the course of three months, we trained about 700 officers.

And every NYPD officer has an iPhone, so we leveraged that resource. We built an app that allowed officers to collect basic information about the type of crime and how it was carried out. Using the app, officers have to answer four questions in a drop-down box:

- What is the category of the crime?
- How was the victim contacted?
- How did the victim pay?
- What contact method did the victim use to pay?

Once they answered the four questions, the app gives them questions to ask the complainant.

The point of the pilot was to teach patrol officers how to gather the key information and write it down, so that the detectives had usable leads to follow when they received the cases.



The screenshot shows the NYPD app interface. At the top is the NYPD logo and the text "New York City Police Department". Below that, a message reads: "Please select the appropriate elements using the dropdown menus below, then click Submit. The questions to ask the C/V will then appear." There are four dropdown menus, each with the text "Please select an answer" and a downward arrow. The questions are: "What is the category of the crime?", "How was the victim contacted?", "How did the victim pay?", and "What contact method did the victim use to pay?".

A friend and I developed the app ourselves, and we have made it open and free to all law enforcement and no one else. I've already distributed it to several small agencies.

One of the first calls I went to was a kid in Queens who had sold his iPhone on eBay, and had left an intimate video on that phone. The person who bought that phone tried to extort him for \$1,000, saying that otherwise the video would be posted on Facebook. The kid was very upset and called the police.

To investigate a case like that, you don't need any forensics. Somebody just had to send a subpoena to eBay and ask who bought the phone. It's quite simple.

But it never gets to that point if the cops don't ask the right questions. The app and the training helped them ask the right questions.

Over the course of the pilot, we found a couple interesting things. First, our estimate of the costs of these crimes rose to \$329 million in 2019.

The second thing we learned is that the demographic profile of victims is across the board. The median age of victims who reported their crime was 42. Older people tended to fall for scams like, "Your nephew is in jail, and you have to send bail money for him." Younger people tended to be victims of extortion, like that kid in Queens. But the demography was evenly spread. Whether you're black or white, rich or poor, it affects everyone in the city.

Deputy Chief Hart

The training, the app, and the presence of the pilot led to much better initial reports. Most cops understood what they were doing. During the pilot program, 60% of the reports had the right terminology and the right details. And 90% of the cops who responded to these types of calls used the app, which I think is a significant accomplishment. We gave them a tool, and they made use of it right away.

We put this out, then everything came to a screeching halt a year ago with COVID. So we don't have as much information about arrests, though we know about some isolated successes. Now we want to get back to focusing on this.

TRAINING

Christina Soto, Intelligence Research Specialist

We started training officers through this pilot program. We started by defining cybercrime, because they often don't know the definition. We explained the categories of complaints. We provided a 1-800 number they could call with questions, and gave them the app. These resources allow them to feel comfortable with these complaints and know that someone in the department is looking at them. After the training, they were much more receptive toward the pilot program.

Deputy Chief Hart

We trained every cop on every patrol tour in every command in Queens South. We wanted to hit all the cops with a short, pointed training at their roll calls. This was 15 minutes in person, in front of the roll call.

IMPLEMENTATION IN SMALLER AGENCIES

Deputy Chief Hart

There's nothing to stop this from being implemented in smaller agencies. Whatever your size, you have trainers. It's not so complex that a local trainer can't teach it in an effective manner.

It helps to have a resource for cops to reach out and ask questions in the moment, whether that's a fusion center or something else. That's one area where it may be harder for a smaller agency to find the resources. But our whole team for this was only about six people.

Christina Soto

Agencies of any size can have analysts review their data for key words to identify hot spots and trends. Agencies can also start training officers at the academy. That training could include defining cybercrime, which types of complaints constitute a cybercrime, and what they should do when they receive a cybercrime complaint.

ADDRESSING CYBER-NATIVE CRIMES



Ravi Satkalmi, Deputy Director for Intelligence Analysis

The NYPD is looking to improve on the intelligence aspect of this problem. For both cyber-enabled and cyber-native crimes, we're learning what the threats look like and coming up with the program to respond to the threats.

Our Intelligence Bureau is closely working with our Information Technology Bureau, which is doing the front-line defense. We're speaking with them on a daily basis to look at the kinds of cyber-native threats toward the NYPD and its systems. That might be people trying to make unauthorized intrusions or a denial-of-service attack. We want to get a sense on who those actors are, how prolific they are, and the danger they present.

We're looking at a range of actors. At the top level, we have highly publicized attacks from nation-states against American entities in government and law enforcement. We also have amateurish folks who go online, purchase malware, and deploy it against a target. That's becoming easier, and we want to understand how we can respond to that.



Lieutenant Gus Rodriguez, Intelligence Bureau

A few detectives and I are assigned to a cyberterrorism squad within the New York City FBI Office's cybercrime task force. We have a guiding question: In the cyber realm, how do we proactively protect the 17 sectors of critical infrastructure that make New York City move? Those sectors include the Department of Environmental Protection, which pumps 1.1 billion gallons of water into the city every day; the Metropolitan Transit Authority, which runs our 26 train lines; and the Department of Transportation, which makes sure our 13,000 traffic lights are working.

Working with those sectors, we realized we needed to pass information about malware we were seeing on to the NYPD's Information Technology Bureau, which has to make sure we respond to 25,000 9-1-1 calls a day. We see the threats day-in and day-out, and we have to make sure that information gets to the NYPD and the other 120 agencies in the city.

MOVING FORWARD

Deputy Chief Hart

This problem is real, and it's affecting our citizens, not far-off places. It's a large amount of money. And we can make a difference if we train our people the right way and give them the right tools.

NPR reported on the pilot program, and we've written a full internal report on the program.

The PERF Critical Issues Report is part of the [Critical Issues in Policing](#) project, supported by the [Motorola Solutions Foundation](#).



**MOTOROLA SOLUTIONS
FOUNDATION**


PERF also is grateful to the [Howard G. Buffett Foundation](#) for supporting this work.

THE HOWARD G.
BUFFETT
FOUNDATION

© Police Executive Research Forum

1120 Connecticut Ave. NW Suite 930 Washington, DC 20036

(202) 466-7820

Back to top 

powered by  MemberClicks