CRITICAL ISSUES IN POLICING SERIES

The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime

POLICE EXECUTIVE RESEARCH FORUM

Page intentionally blank

CRITICAL ISSUES IN POLICING SERIES

The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime

April 2014

POLICE EXECUTIVE RESEARCH FORUM

This publication was supported by the Motorola Solutions Foundation. The points of view expressed herein are the authors' and do not necessarily represent the opinions of the Motorola Solutions Foundation or individual Police Executive Research Forum members.

Police Executive Research Forum, Washington, D.C. 20036

Printed in the United States of America

ISBN: 978-1-934485-24-8

Cover and text page design by Dave Williams.

Cover photo by Alexskopje, licensed by Pond5.com. Other photos by James McGinty.

Contents

Acknowledgments

POLICING HAS ALWAYS BEEN AN EVOLVING profession, but technological advancements in the past 20 years have accelerated that change and dramatically altered the landscape of crime. Police departments are now expected to protect their community members from local offenders committing "traditional" crimes, as well as computer hackers 10,000 miles away. This new cyber threat has developed so quickly that local police agencies haven't had time to fully prepare themselves and identify their role in preventing cybercrime and investigating crimes that are committed.

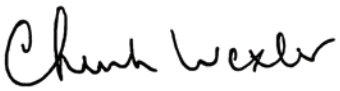
After speaking with several police chiefs about the challenges of cybercrime, we brought this issue to the Motorola Solutions Foundation as a possible project for our Critical Issues in Policing Series. The Motorola Solutions team recognized the importance of this issue and gave it their full support.

The result is this report—the 25th in the Critical Issues series supported by the Motorola Solutions Foundation. I am deeply grateful to our colleagues at Motorola Solutions for their steadfast support of the law enforcement profession, and especially for their commitment to helping us to identify best practices on what I call "the issues that keep police chiefs up at night." I am grateful to Greg Brown, Chairman and CEO of Motorola Solutions; Mark Moon, Executive Vice President and President, Sales and Product Operations; Jack Molloy, Senior Vice President, North America Government Sales; Domingo Herraiz, Vice President, North American Government Affairs; and Matt Blakely, Director of the Motorola Solutions Foundation. I'd also like to thank Rick Neal, retired Vice President at Motorola Solutions and a driving force behind many of PERF's Critical Issues projects.

PERF would not be able to produce our research and summarize the expert views of the leaders in policing without the support of our members. Our daily contacts with PERF members across the nation provide the "finger on the pulse" of policing. In the case of our cybercrime project, PERF members helped us to identify cybercrime as a pressing issue; they provided the information in our cybercrime survey; and they came to Washington to participate in our Summit and tell us what is happening on the ground with respect to cybercrime. As always, I am very grateful to all our members for supporting everything that PERF does.

Finally, I'd like to thank all the people at PERF who contributed to this project. Chief of Staff Andrea Luna and Deputy Chief of Staff Shannon Branly skillfully oversaw this project from beginning to end. Research Assistant Jacob Berman began background work on the subject, and Research Assistant Chris Coghill, Research Associate Jason Cheney, and Project Assistant Balinda Cockrell conducted phone interviews, performed background research, and arranged our Summit. Research Director Rob Davis, Deputy Research Director Bruce Kubu, and Research Assistant Nate Ballard performed the work on our cybercrime survey. Communications Director Craig Fischer and Communications Coordinator James McGinty put together this final publication based on an initial draft by Chris Coghill, and James took the photographs found in this report. And our Graphic Designer, Dave Williams, created the final product you are reading now.

I hope you find this publication to be a clear and concise description of the state of the field and a guide to developing your department's cybercrime capabilities.



Executive Director
Police Executive Research Forum
Washington, D.C.

Cybercrime: A New Critical Issue

By Chuck Wexler

I THINK IT'S SAFE TO SAY THAT AS A GROUP, police chiefs are not given to exaggeration or being alarmist. Most chiefs have seen a lot of things in their lifetime, and they're pretty unflappable.

But at PERF's Cybercrime Summit, the police chiefs and other experts stood up, one after another, to tell us that cybercrime is changing policing, because it allows criminals on the other side of the world to suddenly become a problem in your own back yard. Participants at our Summit went on to say that victims often don't even know where to go to report these crimes, and that local police are struggling to know how to respond.

It was a little startling to hear these stark assessments of the situation, and to hear the frank admissions that most local police agencies have not yet gotten a firm grip on the problem.

Several facts provide a rough idea of the seriousness of this issue:

We don't have anything close to an accurate picture of the problem. The Internet Crime Complaint Center (IC3), a joint effort by the FBI and the National White Collar Crime Center, is the best source of information about the extent of Internet crime. In 2012, the most recent year for which national statistics are available, IC3 received nearly 290,000 complaints from victims who reported total losses of $545 million.[1]

But the head of the FBI's Cyber Division, Joe Demarest, told us that he estimates that only about 10 percent of all incidents are reported to IC3. Banks often find it less expensive to simply reimburse victims whose bank accounts are drained by cyber-thieves, in order to avoid publicity about their protective systems failing. So it may never occur to most victims even to report the crime, because they call the bank and the bank "takes care of it."

However, what we do know is cause for concern: One international event in 2013, involving thefts from ATM machines over a 10-hour period, resulted in losses of $45 million—more than the total losses from all "traditional" bank robberies in the United States over the course of a year.[2] At the local level, police chiefs are noticing that gangs are switching from illegal drug sales to cyber-scams to generate money, because cybercrime is easier and safer for the criminals.

We have not yet developed solutions to certain aspects of the problem: Many experts noted that cybercrime creates jurisdictional problems, because the perpetrator often lives thousands of miles away from the victim. As one local police executive put it, "Our closure rates are below 10 percent, because I can't call a police department or prosecutor 800 miles away and ask them to invest all these resources to bring a criminal to our jurisdiction to be charged with a crime."

---

1. "2012 IC3 Annual Report." http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf
2. In Hours, Thieves Took $45 Million in A.T.M. Scheme. *The New York Times,* 9 May 2013. http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?pagewanted=all

Often, low-level offenders are operating unchallenged: The FBI, Secret Service, and other federal agencies are focusing their limited resources on the largest cases. Cybercrimes involving losses of $500 or less are often considered too small even for local police to investigate, much less federal agencies, because of the jurisdictional issues and other challenges. Many local police executives acknowledge that currently they are "behind the curve" in finding a role for their agencies with cybercrime.

Despite all of these challenges, we must take on cybercrime. As of early 2014, the government has staked out a major role for law enforcement *at the federal level.* But most of the 18,000 local and state law enforcement agencies have not yet developed plans and jurisdictional authority to enter this arena. This report is a wake-up call to state and local police leaders to get in the game. Crime is changing, and policing must change too. While overall crime in the United States is down almost to 1960s levels, cybercrime is increasing. Local and state governments must recognize that the crime-fighting successes of these past 50 years are not preparing us for the new crimes of this millennium.

This report aims to describe what police chiefs and other experts are currently identifying as best approaches. We need dramatic increases in awareness of the issues, by the public and by the police. Local police agencies must identify roles for themselves. Elected officials must increase resources for fighting cybercrime. And we will probably need new laws to handle the jurisdictional issues.

The bad news is that it's the bottom of the second inning, and our team is behind about 12 to 1. The good news is: It's only the bottom of the second inning, and we're getting warmed up. The game is just beginning.

This report is a wake-up call to state and local police leaders to get in the game. Crime is changing, and policing must change too. While overall crime in the United States is down almost to 1960s levels, cybercrime is increasing. Local and state governments must recognize that the crime-fighting successes of these past 50 years are not preparing us for the new crimes of this millennium.

The Nature of the Challenges

ON SEPTEMBER 10, 2013, PERF HELD AN *executive-level Summit for law enforcement practitioners on the local police response to cybercrime. Participants in the PERF Summit described the evolving nature of the cybercrime threat, including how nearly every type of "traditional" crime today can contain cyber aspects. For example, many police departments are reporting that smart phones have become the most common item taken in street robberies. And the GPS tracking software in smartphones and computers often provide police with leads for investigating robberies and burglaries.*

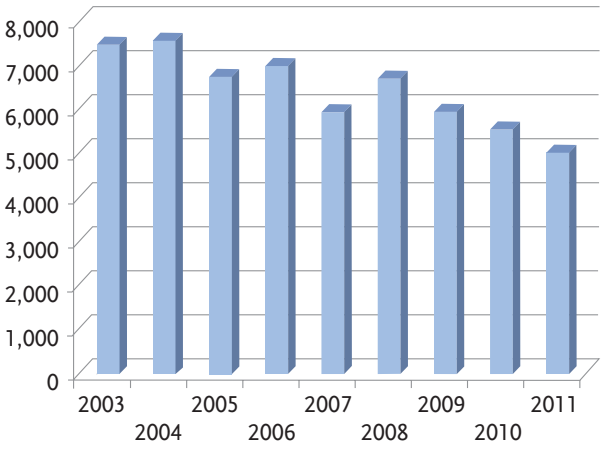
In many ways, cybercrime is a new kind of threat. Cyber-criminals can commit crimes against victims who are thousands of miles away. So people today are vulnerable to threats from criminals who would never have had access to them 20 years ago. It is easier for cyber-criminals to hide from the police, because in some cases they never show their face to the police or even to victims.

In other ways, cybercrime is a new means to commit crimes police have dealt with for decades. Fraud committed over the Internet is still fraud. Sex traffickers use social media to advertise prostitution. Street gangs increasingly are generating income by selling fake tickets to sports or musical events.

Cybercrime can have significant impacts. As police succeed in preventing traditional crimes such as bank robberies, those gains are dwarfed by increases in cybercrime:

Bank robberies decrease...

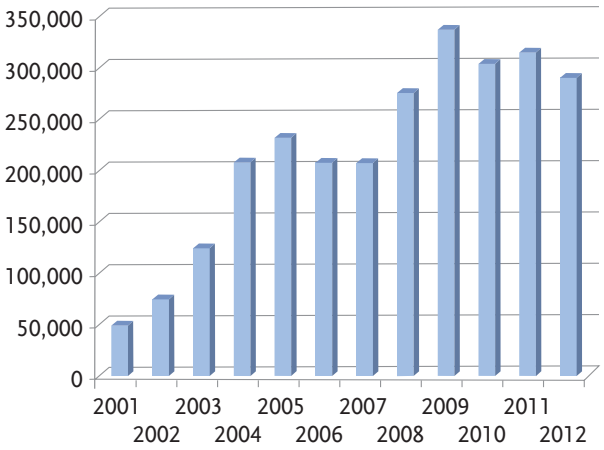
TRADITIONAL BANK ROBBERIES



Data from FBI Bank Crime Statistics (BCS) Report

...while cyber attacks increase

NUMBER OF COMPLAINTS REPORTED TO IC3



Data from IC3 Annual Reports

Cybercrimes aren't always about monetary loss to the victim. A Florida 12-year-old committed suicide in September 2013 after allegedly being cyber-bullied by a 12-year-old and 14-year-old. Polk County Sheriff Grady Judd charged the two girls with stalking, but prosecutors eventually dropped the charges.[3] Schools across the country are struggling with cyber-bullying.

A number of participants at PERF's Cybercrime Summit said that local law enforcement agencies need to step up their response to this issue. Cybercrime has evolved at an astonishing rate, and for a number of reasons cited below, many police agencies are not equipped to take a large role in cybercrime investigations. But participants expressed confidence that police will "catch up" and identify their best roles in the prevention and investigation of cybercrime, if for no other reason than that the public is demanding it.

Following are comments made by participants at PERF's Summit about the state of cybercrime and local police agencies' response:

Executive Director Michael Kaiser, National Cyber Security Alliance:

Almost Every Crime Has a Technological Aspect

Almost every crime in your community has a technological aspect now. I would guess at least 80 percent of crimes have a cyber aspect—a voicemail, a Facebook post, data from a cell phone call. Even for an investigation into something simple, like a street robbery, detectives often need to look into data from a stolen cell phone, including GPS data that can show exactly where the phone is located, often within a matter of 10 or 20 feet. I think this demonstrates the importance of having police departments prepared for this type of crime.

Chief Cathy Lanier, Metropolitan Police Department, Washington, D.C.:

Police Need Proficiency In Three Areas of Cyber-Intelligence

I see three different sets of cyber-skills that police departments need to become proficient in handling. The first is what most of us think of as cybercrime: the criminal acts that are committed using the Internet. This includes things like prostitution, human trafficking, and identity theft. Some are entirely Internet-based while others are more "traditional" crimes that have a cyber element.

The second is crime prevention. We need to use cyber-intelligence gathered from sources like open-source social media to prevent crime. There are vast amounts of data available that can help us predict what is coming, if we know where to look for it.

The third piece of cybercrime is the investigative element. Whether we like it or not, right now something as simple as investigating a basic street robbery requires your detectives to have technological expertise. Any investigation could include GPS, different kinds of digital video, metadata, and social media.

Those are the three very distinct areas in my mind, and I think most of us are struggling with all of them.

Washington, DC Metropolitan Police Chief Cathy Lanier

3. "Charges dropped against girls in Florida cyber-bullying case." *NBC News,* 20 Nov 2013. http://www.nbcnews.com/news/us-news/charges-dropped-against-girls-florida-cyber-bullying-suicide-case-v21551488

BJA Director
Denise O'Donnell

President/CEO Maria Vello,
National Cyber-Forensics and Training Alliance:

Every Device You Use Makes You Vulnerable to Cybercrime

Almost everyone takes part in the digital lifestyle these days. When I look around this room, I see everybody on their wireless devices—laptops, tablets, smartphones. Do you know who else is tapping into that wireless connection you are using? Do you know whether anybody can look at what you are doing, or read that email you're sending right now? I think everyone, including the police officials in this room, have to be more aware of how people can gain access to our data.

Bureau of Justice Assistance Director
Denise O'Donnell:

DOJ Wants to Know How It Can Best Support Local Police

Cybercrime isn't just a "new thing"; it is the future of law enforcement. Computers and the internet are now universally used to facilitate traditional crime from fraud and identity theft to drug and human trafficking; from bullying and hate crimes to attacks on our national infrastructure. Going forward, this will be the biggest problem in much of what you do as police.

We at the Bureau of Justice Assistance look forward to hearing from you about how we can support state and local law enforcement, to the extent that we have resources you can use. We'd like to know the most important things that we can do to support you, in addition to the training that we already have under way.

How Criminals Are Committing Cybercrimes

Participants at PERF's Summit reported that criminal organizations are turning to cybercrime to finance their operations. Criminals and gangs have learned that cybercrime puts them at less risk for arrest or injury, and can earn them more money, than selling illegal drugs or committing other street crimes.

Chicago Police Detective Patricia Dalton:

Gangs Can Make $30,000 a Month Making Fake Credit Cards And Other Cyber Scams

In Chicago we have found that organized gangs now make more money from financial crimes than they do by selling drugs on street corners.

One way they do this is by purchasing a set of credit card numbers on the Internet, and either re-encoding the cards or making new cards, embossing a name on the front of it, making matching fake IDs, and buying gift cards in stores.

We also have people running a ticket scam right now by trolling Craigslist for people who will buy counterfeit tickets to concerts or sports events. They create counterfeit tickets on the computer and then see who they can scam online.

Our confidential informants have told us that these people make approximately $30,000 a month,

and that is for each group that is out there operating. It's easy, so these criminals are enthusiastically getting involved.

We see a lot of cybercrimes being perpetrated by local offenders, most of whom are gang members. This is concerning to us, both because of the loss to the victim and the income for the gang.

Minneapolis Chief Janeé Harteau:

Cybercrime Is Safer for the Criminal And Harder for the Police

We are beginning to see gang members do the same things that were described from Chicago. It is much

Chicago Detective Patricia Dalton

Results of a PERF Cybercrime Survey

In August 2013, PERF conducted a survey of 498 law enforcement agencies to examine the role of local police in combating cybercrime. 213 agencies responded, for a 43 percent response rate.

PERF found that agencies use different definitions of cybercrime. For this survey, cybercrime was defined as a range of crimes involving: (1) the use of computers, smartphones, tablets, or other electronic devices as tools to commit a "traditional" crime such as theft or fraud; (2) the use of computers to commit online crimes, such as hacking, stealing data, and spreading computer viruses; and (3) the use of computers for storage of illegal material, such as child pornography.

Definitions and Criminal Codes: 13 percent of responding agencies said they have an official definition of computer or cybercrime, and 84 percent said they have specific state or local criminal codes governing computer crime and/or cybercrime. 25 percent of responding agencies said they analyze data on cybercrimes to identify trends and/or guide investigations.

PERF asked agencies to list the criminal codes they most frequently use when charging cyber-specific crimes. The most common responses, in descending order, were: child exploitation, unlawful access to computer/networks, fraud, harassment/stalking, identity theft, and general "computer crime."

Thus, the most common area of cybercrime investigations by local police continues to be their longstanding role in protecting children against pornographers or other threats.

Computer/Cybercrime Personnel: 42 percent of responding agencies reported having a computer crime or cybercrime unit. Among those agencies, 92 percent of the computer crime units involve evidence recovery (such as tracking stolen laptops); 46 percent conduct mobile phone tracking; 45 percent perform video enhancement (such as security camera footage); and 62 percent conduct analyses of social media

easier to fund gang efforts through cybercrime than it is to rob somebody or sell drugs on the street corner, because you are much less likely to get caught. We can't physically see these cybercrimes, so there's less evidence, and less risk to the criminal.

FBI Supervisory Special Agent Herb Stapleton:

Gangs Are Filing Fraudulent Tax Returns

The Internet Crime Complaint Center (IC3) has received numerous complaints about gangs committing cybercrimes. Filing fraudulent tax returns in order to get tax "refunds" has been a particularly popular way for gangs to finance their organizations.

Minneapolis Chief Janeé Harteau

for investigative purposes. Other functions that agencies listed in their responses include computer and mobile phone data forensics and child exploitation/pornography prevention, including monitoring websites and networks.

Of the agencies with a computer crime or cybercrime unit, 96 percent provide those personnel with specialized training; 37 percent use in-house training; 80 percent use a regional or statewide specialized program for training; and 63 percent use an outsourced training provider.

Outsourced training providers mentioned by survey respondents include the National White Collar Crime Center, Encase, Access Data, the U.S. Secret Service, Guidance Software, the FBI, the Internet Crimes Against Children Task Force Program, the Department of Homeland Security, and the International Association of Cyber Investigative Specialists.

Challenges to Investigating Cybercrime: Departments were asked about the three biggest challenges to investigating cybercrime in their agencies. Of agencies that responded, 54 percent said a lack of staffing; 31 percent said a lack of funding; and 29 percent said a lack of in-house expertise.

Case Referrals: The FBI and the U.S. Secret Service are the agencies that most often receive referrals of cybercrime cases from local police. The PERF survey found that 66 percent of responding agencies refer cases to the FBI, and 51 percent to the U.S. Secret Service. In addition, 21 percent of agencies refer cybercrime cases to a local task force; 32 percent to a state task force; 30 percent to a federal task force; 35 percent to another local jurisdiction; and 25 percent to other agencies.

Other Survey Findings: 18 percent of responding local police agencies have themselves been the *victim* of a cyber attack. 49 percent of responding agencies take specific actions to prevent cybercrime, such as actively looking for illegal cyber activity or offenders, rather than solely responding to reported crimes. 68 percent of responding agencies participate in cybercrime prevention initiatives or educational campaigns, to help community members protect themselves against becoming victims of cybercrime.

John Cohen, Principal Deputy Under Secretary for Intelligence & Analysis And Counterterrorism Coordinator, DHS:

Perpetrators Use the Internet To Commit Traditional Crimes

In the counter-terrorism world we are seeing a blend of cyber and non-cyber activities, especially when it comes to potential mass casualty attacks or attacks on critical infrastructure. We're seeing criminal organizations and individual perpetrators, both in the United States and abroad, use cyber-intrusion techniques to obtain information about individuals, events, or facilities. Their purpose isn't to commit a cyber attack on these targets, but to better inform their physical attacks on these targets.

For example, in many recent mass shootings around the country, including the one in Aurora, Colorado, perpetrators obtained information through the Internet about the tactics and equipment they used to carry out their attacks.[4] Information about who accesses this kind of information is available to us in law enforcement if we know how to look for it.

John Cohen, Principal Deputy Under Secretary
For Intelligence & Analysis
And Counterterrorism Coordinator, DHS

The Impact of Cybercrime

Executive Director Michael Kaiser, National Cyber Security Alliance:

Cybercrimes Hurt Small Businesses

The small businesses in your communities are a prime target for a lot of cyber-criminals. The $100-million cases get the most attention, but the majority of cyber-criminals are going after the businesses in your community. Most attacks happen to companies with fewer than 1,000 employees. Sixty percent of the businesses targeted in those attacks go out of business within six months. They don't have the resources to respond to the cybercrimes themselves, or the capital to absorb the losses.

And that isn't always because of the loss of money. Money is certainly an important and tangible loss in many cybercrimes, but data is often the more important target. Many people steal information and intellectual property, or they try to steal consumer data.

Toronto Deputy Chief Peter Sloly:

Local Police Agencies Must Get in the Game

The stories about these $45-million ATF crimes blow your mind, but many cybercrimes are about more than money. For example, if a young woman is sexually assaulted, and then bullied about it online, which causes her to take her own life, how do local police respond if they have little or no capacity, understanding, or ability to investigate the

continued on page 10

4. The alleged perpetrator of the July 20, 2012 shooting in an Aurora, CO movie theater used the internet to purchase and stockpile the weapons, ammunition, and protective equipment used in the attack. (Associated Press, July 23, 2012. http://www.myfoxaustin.com/story/19091698/colorado)

Cyber Criminals Steal Data from Millions of Credit and Debit Cards

In late 2013 and early 2014, criminals stole data from millions of credit and debit cards by exploiting a weakness in the credit card processing pads at several major U.S. retailers. The largest data breach occurred at Target, where criminals took records from over 40 million payment cards and personal information regarding 70 million customers.[5] At Neiman Marcus, information from 1.1 million payment cards reportedly was stolen from July to October 2013.[6] Similar thefts have also been reported at Michael's stores and Sally Beauty.[7]

The costs of these crimes have fallen on everyone involved—retailers, consumers, and credit card companies. The financial costs are the responsibility of credit card companies, which can sue retailers if they feel the breach occurred because the retailers' security systems were not sufficient.[8] In 2007, 45 million payment cards were stolen from T.J. Maxx, and the company reportedly settled with Visa for $65 million. Credit card companies have also had to handle the costs of reissuing cards, a cost that Bloomberg Businessweek estimates at $400 million for the Target breach. JPMorgan and Citibank reissued all debit cards that were compromised in the Target data theft.

In addition to any financial liability they may have, retailers also face the loss of consumer confidence that comes with major data breaches. And while customers are not liable for the fraudulent charges made as a result of data theft, many have spent hours getting their finances back in order and temporarily did not have access to funds that should have been in their accounts.

Some potential solutions have been discussed, including the use of embedded chips instead of magnetic strips to read the information on a credit card.[9] These cards also require consumers to enter their personal identification number (PIN) into a keypad to verify their identity. These chip-and-PIN cards are common throughout the rest of the world, but the United States has been slow to commit to the massive undertaking of changing all the credit cards and credit card readers in the country.[10]

---

5. A Sneaky Path Into Target Customers' Wallets. *New York Times,* January 18, 2014. http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html

6. Neiman Marcus Data Breach Worse Than First Said. *New York Times,* January 24, 2014. http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html

7. Sally Beauty Investigating Possible Credit Card Theft. *New York Times,* March 5, 2013. http://bits.blogs.nytimes.com/2014/03/05/sally-beauty-investigating-possible-credit-card-theft/

8. Who Should Pay for Data Theft? *Bloomberg Businessweek,* February 20, 2014. http://www.businessweek.com/articles/2014-02-20/who-should-pay-for-data-theft

9. Experts warn of coming wave of serious cybercrime. *Washington Post,* February 9, 2014. http://www.washingtonpost.com/business/economy/target-breach-could-represent-leading-edge-of-wave-of-serious-cybercrime/2014/02/09/dc8ea02c-8daa-11e3-833c-33098f9e5267_story.html

10. A chip and a PIN: The future of credit cards. *Fox News,* February 10, 2014. http://www.foxnews.com/tech/2014/02/10/chip-and-pin-future-credit-cards/

continued from page 8

crime? The crime may go unsolved and become a huge issue of community trust. And if it grabs attention on the Internet, cyber-vigilantes may decide to come in and use their capabilities to investigate the crime online. It shines a spotlight on the inability of the police to investigate these sorts of cases. Just about every type of human interaction can have this type of cyber-victimization now. Beyond the big-dollar cases, cybercrime is part of every crime now, and we in law enforcement have to be in this game.

John Cohen, Principal Deputy Under Secretary for Intelligence & Analysis
And Counterterrorism Coordinator, DHS:

Cybercriminals Also Target Police Departments

In March 2013, DHS issued a warning to law enforcement agencies about Telephony Denial of Service (TDoS) attacks against government public safety organizations. These TDoS schemes flood a public service agency's phone lines with constant phone calls, preventing the agency from making or receiving calls. The perpetrators attempted to extort money from the organizations for agreeing to stop the calls. Multiple jurisdictions reported being victimized by this type of attack.[11]

There have been a number of cases where organizations based abroad or in the United States have committed denial-of-service attacks against police agencies. Their goal was to disrupt the ability of the police departments to take phone calls from the public, and in some cases they have been able to take a department completely offline.

We are also seeing web defacement, in which a group of individuals redirect traffic from your website to a website that they control, and create erroneous or problematic messages regarding your organization.

11. DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs. *National Emergency Number Association.* March 17, 2013. https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm.

Challenges in Confronting Cybercrime

PARTICIPANTS AT THE PERF SUMMIT DISCUSSED *recurring challenges that police departments face when addressing cybercrime, including the underreporting of crimes by individuals and corporations, inadequate awareness of this issue by public officials and the public, the sometimes overwhelming scale of these crimes, and difficulties in handling crimes that stretch across multiple jurisdictions.*

Failures to Report Cybercrimes To Police

Consumer trust is vital for private-sector corporations, so data breaches can be catastrophic for business. As a result, when cybercriminals take money from a victim's bank account or make fraudulent charges on a victim's credit card, the banks or credit card companies often reimburse the victim for the losses, rather than suffer bad publicity about their customers being victimized.

While this approach makes the situation easier for the victim and it may make sense for the businesses, there are significant disadvantages. If the victim's first phone call is to the bank and the bank quickly reimburses the victim, the victim may never even think to report the crime to the police. If the crimes are never reported, they are not investigated by law enforcement agencies or counted in crime statistics. And the perpetrators remain free to commit more crimes.

Houston Chief Charles McClelland:

Private Companies Don't Want To Admit They've Been Hacked

Businesses are being hacked or victimized, but they won't report it because they don't want to undermine consumer confidence. That is why the bank is willing to put $500 back into a customer's account rather then tell 500,000 customers that their information may have been compromised. Often we will know that a certain corporation's databases have been compromised, but when we ask them about it, they won't cooperate.

They look at their bottom line and assume that no one will want to do business with a company with a track record of having their customers' information compromised.

Detective Chief Superintendent Paul Rumney, Greater Manchester Police:

Traditional Crime Measurements Underemphasize Cybercrime

We've been trying to get a handle on the extent of the problem, but it's been difficult for us. Traditionally our crime measurements include things like burglary, theft, robbery, and rape. Most cybercrime we have experienced to date is a traditional crime such as fraud, theft, harassment, or blackmail enabled by the use of a computer, and as such we have recorded it as a traditional crime. We will soon begin recording cyber-enabled crime specifically, and we'll gain a better understanding of the scale.

Greater Manchester, UK Detective Chief Superintendent Paul Rumney

Making Cybercrime a Priority

Houston Chief Charles McClelland:

Violent Crime Is Seen As a Higher Priority than Cybercrime

I think cybercrime has been low on the priority list for us for two reasons. The first is a lack of knowledge of how widespread this type of crime is. The second is that we have to use our resources efficiently, and when you have blood running down the street like we do in some of our major cities, addressing those violent crime problems is our priority. That's what people see every day and expect us to address.

Los Angeles County Chief William McSweeney:

We're Making the Transition To Deal with Cybercrime

I think that almost all local police agencies have a bit of a cultural problem that gets in the way of dealing with these issues. It's been an awkward shift towards handling cybercrime, and many local agencies have been slow to embrace this part of the job.

Houston Chief Charles McClelland

We'd much prefer to see federal agencies handle it. Culturally, we'd prefer to handle old-fashioned crime and wish this wasn't becoming an issue.

Unfortunately, we haven't properly prepared our officers to handle cybercrime calls. Our agency receives a hundred calls a day for cybercrime complaints, and too often the responding officers basically just gave the victim a blank stare or gave them a minimal answer to finish the interaction as quickly as possible.

We need to prepare our officers to respond to these calls, give sound advice, and write a thorough report. When people report a crime and get a blank stare because the officer doesn't understand how the crimes are committed and what can be done, public confidence in police agencies deteriorates, and people will stop turning to us to solve their problems.

But I think we're beginning to realize that cybercrime is here to stay, and we're making the transition.

Indianapolis Public Safety Director Troy Riggs

Executive Director Darrel Stephens, Major City Chiefs Association:

Current State Laws Are Inadequate

Current state-level laws don't address many of the kinds of situations that our police agencies are encountering. That leaves the feds as the only people with authority to investigate. But many of the crimes we see aren't big enough to reach the threshold of what the federal agencies will handle, because they are focusing their resources on the large cases.

Toronto Deputy Chief Peter Sloly:

Cybercrime Must Be a Priority Because It Impacts Everything We Do

It's not about looking at cybercrime *as opposed to* other crime. We all have to recognize that there's a cyber, social and digital element to just about every crime and police operation in which we are involved. I think by looking at it that way, we can recognize that this is a priority issue.

Special Agent in Charge Ed Lowery, U.S. Secret Service:

Every Crime Is Facilitated by Cybercrime

We need universal awareness and understanding that the world has changed. Most crime that we investigate is facilitated through cyberspace. Everyone needs to be aware of that and needs to accept that some of our younger employees are a lot more aware of what's going on in this realm than we are.

Indianapolis Director Troy Riggs:

One of Us Will Probably Be in Charge When the Next Major Cyberattack Occurs

We need to be proactive and prepared, especially because it's likely that someone in this room will be in charge when the next major cyber attack occurs in our country. My department has begun taking the first steps to prepare ourselves. And we don't want to wait until something happens to prepare ourselves for this. If it's an issue of funding, we need to make the case to our city councils and citizens that this is a priority for us.

MCC Executive Director Darrel Stephens

Scale of the Crimes

Los Angeles County Chief William McSweeney:

Federal Agencies Take the High-Loss Cases And Leave Smaller Cases to Local Police

One thing we haven't addressed yet is the volume of cases. There are so many cases that federal agencies skim off the high-loss cases, leaving local agencies with smaller things like forged tickets to sports or music events, losses of less than $1,000, or other relatively small scams. The volume of these cases would be way too much for federal agencies to handle.

We need to either decide that we're going to empower and properly equip local police to take on these crimes, or decide that we're going to ignore them, which, for the most part, is what we're doing now.

FBI Assistant Director Joe Demarest:

We Are Working with State and Local Police To Get Them the Skills They Need

There are no borders on the Internet, and many of the people we're interested in for both criminal and national security reasons are overseas. When local police face cases like that, they may not have the time, personnel, or resources to address these issues. We're working closely with state and local agencies to get them the skills and capability they need.

Jurisdictional Issues

Police departments increasingly are finding that their community members are being victimized through cybercrime by someone across the country or on the other side of the world. Often it is difficult even to establish which police agency has jurisdiction over these crimes.

New York City Captain Michael Shugrue:

Cybercrime Opens the Whole World To Your Jurisdiction

Cybercrimes essentially reduce the size of the world, so that someone across the globe can become part of your jurisdiction. Traditionally, our focus has been on people within our municipal borders. But on any given day, it may be more important for the NYPD to address a problem caused by someone in Sri Lanka than by someone in Brooklyn.

It has made the world a much smaller place for law enforcement.

Ramsey County, MN Inspector Robert Allen:

Extraditing Offenders To a Different Jurisdiction Often Isn't Feasible in Low-Dollar Cases

I think jurisdictional issues are one of the huge challenges with cybercrime. Our Minneapolis-St. Paul metropolitan area has 86 local law enforcement

RIGHT:
FBI Assistant Director Joseph Demarest
FAR RIGHT:
NYPD Captain Michael Shugrue

agencies covering nine counties, so we frequently face groups of criminals committing scams that cross into multiple jurisdictions. If we happen to learn about them through confidential informants and start investigating what they are doing, we often find that their crime activity might not be happening in our jurisdiction. The loss is often occurring hundreds of miles away.

When the amounts of those losses are significant, we can transfer them to a regional task force. But we don't always have the resources to handle the smaller losses—$500 or $1,000—and those cases are the ones where we are not serving our citizens well. Even if we could investigate them, it may not make economic sense to put the necessary resources into those cases. Other agencies often may not be willing to invest in having those criminals extradited to our county to be prosecuted.

Elk Grove, CA Chief Robert Lehner:

We Need Better State Laws To Govern Interstate Cybercrimes

The jurisdictional issues we have been talking about here are critical. We have had a number of cases where the victim is in our jurisdiction and the suspect is in another state, or vice versa. Even if you have a solid case, where will it be prosecuted? How will it be prosecuted? Our laws don't really support it.

I would like to see a better national and interstate structure to handle these cases. Maybe that would take the form of a set of model statutes that we can advocate for in our individual legislatures, to support enforcement of interstate criminal activity.

Fairfax County, VA Lieutenant Bob Blakley:

Large Cases Are Tackled Immediately, But Small Interstate Cases Are Difficult

In the metropolitan Washington, D.C. area, we are fortunate to have a Secret Service agent embedded with us, which is a very good resource for cybercrimes. With the Secret Service's help, the larger cases are tackled immediately.

But smaller cases, like fraudulent ticket scams,

TOP: Ramsey Co., MN Inspector Robert Allen
MIDDLE: Elk Grove, CA Chief Robert Lehner
BOTTOM: Fairfax Co., VA Lieutenant Bob Blakley

are dime-a-dozen. That is where the local jurisdictions run into a wall on a daily basis. Our closure rates are below 10 percent, because I can't call a police department or prosecutor 800 miles away and ask them to invest all these resources to bring a criminal to our jurisdiction to be charged with a crime. These are the problems that you run into, and the locals have few resources to fix that.

Des Moines Major Stephen Waymire:

We're Sworn to Protect Our Communities

We need to do what we can to protect our jurisdiction. We're going to have problems with crimes that cross jurisdictional lines or even national borders, but we have very real victims whom we are responsible for supporting.

I think we're getting better at working these cases that cross jurisdictional boundaries. And we need to get better at it, because we have to be able to serve the citizens we're sworn to protect, no matter where the perpetrators may be.

Des Moines Major Stephen Waymire

Promising Practices

Task Forces

The USA PATRIOT Act of 2001 established nationwide Electronic Crime Task Forces (ECTFs). Under the ECTF model, local, state, and federal law enforcement agencies work together with prosecutors, private-sector companies, and academic experts to address the "prevention, detection, mitigation and aggressive investigation of attacks on the nation's financial and critical infrastructures."[12]

PERF Summit participants reported that these task forces are one of the most effective ways to deal with cybercrime. Local agencies provide the on-the-ground resources necessary for the investigations, and federal agencies can assist in connecting cases in multiple jurisdictions and investigating large-scale operations.

U.S. Secret Service Special Agent in Charge Ed Lowery:

Task Forces Leverage Partners' Strengths

The Secret Service utilizes the task force approach through our 35 Electronic Crimes Task Forces (ECTFs). The ECTFs allow us to work collaboratively and make sure all members are aware of every situation encountered through our strategic cyber investigations. Some agencies are better suited to handle certain types of cases. In particular, federal law enforcement agencies routinely handle international investigations; however, we often work together with state and local law enforcement on targeted enforcement cases. This task force approach allows us to leverage each agency's strengths in concert, including the FBI, Secret Service, ICE, and state and local agencies.

President/CEO Maria Vello, National Cyber-Forensics & Training Alliance:

Most of These Cases Are Not Isolated Incidents

Everyone in this room needs to work together to find solutions to these problems. Only together can we figure out what's happening. Most of these cases are not isolated incidents. If it's happening at one bank, it's probably happening at another. The same

CEO-President Maria Vello, National Cyber-Forensics and Training Alliance

12. United States Secret Service. "Electronic Crimes Task Forces and Working Groups." http://www.secretservice.gov/ectf.shtml.

RIGHT:
FBI Section Chief
Don Good

FAR RIGHT:
MacAndrews and
Forbes Vice President
Tim Murphy

is true for cyber elements of prostitution, child pornography, drug trafficking, and terrorism. To connect all these dots, everyone needs to collaborate.

FBI Assistant Director Joe Demarest:

Investigating Cybercrime Is a Team Sport

Combating cybercrime is a team sport. Whether it is a local, state, or federal level agency, one agency can't do this alone. We work with other law enforcement agencies, and with the private sector. They often have information we don't. You need to have them on board because they are often the ones who actually help facilitate the investigations.

FBI Section Chief Don Good:

Collaboration With the Private Sector Is Critical

I'm responsible for the FBI's Cyber Operations and Outreach Section. Our focus is outreach to the private sector so we can work more collaboratively on these cases. We in the FBI feel that developing that relationship is key to what we need to do about cybercrime. The private sector comprises approximately 85 to 90 percent of the Internet. Without the cooperation of the private sector, we can't be successful at what we do.

Tim Murphy, MacAndrews and Forbes Vice President and former FBI Deputy Director:

Cybercrime Today Is Similar To Fighting Terrorism after 9/11

Our overarching goal should be to connect all our efforts, as we did with terrorism after 9/11. The task forces we put in place to fight terrorism led to a crowd-sourcing effort within the law enforcement community to prevent and solve these crimes. I think we can do a similar thing here with the law enforcement and private sector communities to get everyone working together on cybercrimes and threats, sharing information in real time.

Henrico County, VA Chief Douglas Middleton:

Task Forces Work Well, But I Still See a Gap in What We Do

We have a great connection with the FBI. We are on their cyber task force; we are on the Internet Crimes Against Children task force; and we work very closely with the Secret Service as well. Our forensic unit handles cybercrime and is staffed with people trained by the Secret Service. We take advantage of any equipment we are offered by federal agencies.

All this is to say that federal agencies have done a lot to help us deal with our cybercrime issues, but I still see a gap in how we're going to handle the cases that are the responsibility of local agencies.

FAR LEFT:
Henrico Co., VA Chief Douglas Middleton

LEFT:
Springfield, MO Chief Paul Williams

My officers are the ones with their boots on the ground, responding to the calls for service. When they answer a call and someone wants to file a complaint about being the victim of a cybercrime, we take the report and do our best to resolve it, but we aren't responding as well as we should be to those complaints.

Springfield, MO Chief Paul Williams:

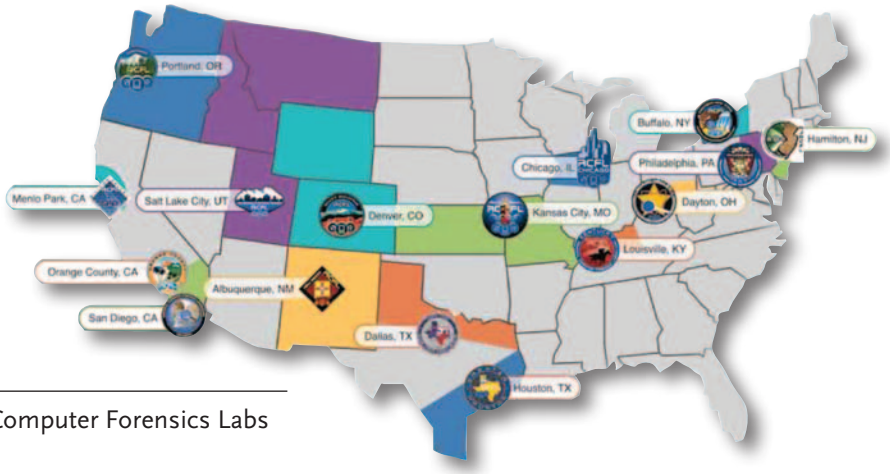
We Created a Computer Forensics Lab

Regional Computer Forensics Labs (RCFLs) are laboratories created by the FBI for the forensic investigation of all digital evidence. There are 16 RCFLs across the United States, each staffed by 12 examiners and three support staff members. Law enforcement agencies within the region can bring their digital evidence to the RCFLs for investigation.[13]

Kansas City has a Regional Computer Forensics Lab (RCFL), but it's 180 miles away from us. Nobody in the southwest part of the state really wants to drive to Kansas City to have their forensic evidence downloaded, so we decided to create a computer forensics lab of our own, and offered up the resources to local law enforcement in the Springfield area.

About half of the forensic lab's staff time was being spent assisting other agencies, so we opened up a little kiosk for the basic tasks. If an officer wants to download data from a cell phone, a laptop, or other common electronic devices, the officer can plug it in, download it, and then take it back with them. If it's something that requires more expertise, the officer can turn the device over to our employees, and we will put it in the queue and work on it as soon as we have some free time.

continued on page 23



Locations of Regional Computer Forensics Labs

13. About RCFLs. *Regional Computer Forensics Laboratory Website.* http://www.rcfl.gov/DSP_P_about.cfm.

Internet Crime Complaint Center (IC3) Asks Local Police: "Please Encourage Victims to Report Cybercrime to Us"

The Internet Crime Complaint Center (IC3) was formed by the FBI and the National White Collar Crime Center in 2000 to receive complaints of web-based crimes. IC3 receives complaints about a wide range of crimes, including fraud, economic espionage, hacking, online extortion, and identity theft.

IC3's staff of about 30 people refers cases to local, state, federal, and international law enforcement agencies and task forces, gathers national statistics on Internet crime, informs police agencies and the public of national cybercrime trends, and issues public service announcements and "scam alerts" regarding current types of fraud that are occurring.[14]

For example, in November 2013, IC3 released a Scam Alert about a type of fraud in which cybercriminals telephone victims and purport to be employees of a major software company. The caller says that the user's computer is sending error messages and that a virus has been detected. The victims are convinced to allow the caller remote access to their computer, and then are asked to pay to have infected files removed. "Whether the users pay for the removal of the virus or not, many reported difficulties with their computers afterward," IC3 said.

FBI Assistant Director Joe Demarest, Section Chief Don Good, and SSA Herb Stapleton spoke with PERF Summit participants about the IC3.

FBI Supervisory Special Agent Herb Stapleton:

IC3 Connects Smaller Cases

IC3 received approximately 25,000 complaints in its first year and now receives approximately 300,000 complaints annually. For those who report a loss, the average loss reported is about $4,500. The majority of victims do not report a loss.

All complaints that come into IC3 are run through a computer system that sorts the complaints and

IC3 flyer

What Is the Definition of Internet Crime?

IC3 provides the following definition of Internet crime:

"Any illegal activity involving one or more components of the Internet, such as websites, chat rooms, and/or email. Internet crime involves the use of the Intenet to communicate false or fraudulent representations to consumers. These crimes may include, but are not limited to, advance-fee schemes, non-delivery of goods or services, computer hacking, or employment/business opportunity schemes."

The IC3 webpage also provides detailed descriptions of various crime schemes, including credit card fraud, debt elimination fraud, identity theft, auction frauds, counterfeit cashier's checks, Internet extortion, escrow services fraud, investment fraud, lotteries, phishing and spoofing, ponzi/pyramid schemes, "Nigerian letters/419 scams," and "third-party receiver of funds" schemes.[15]

14. About Us. *Internet Crime Complaint Center.* http://www.ic3.gov/about/default.aspx.
15. http://www.ic3.gov/crimeschemes.aspx

looks for patterns. When it identifies patterns, they are referred to human analysts who look at the collection of complaints. Our threshold for sending a case packet for investigation is a total of $25,000 in losses.

When this threshold is met, we send our leads to the FBI field offices and appropriate state and local police agencies. We ask those agencies to let us and everyone else who received the lead know if they are pursuing the investigation, but this reporting isn't mandatory. This means multiple agencies could be investigating the same case without knowing it.

I've heard some of the chiefs here say that they're dealing with cases that only involve a $500 or $1,000 loss. I'm sure some of those are isolated cases, but I think most of the smaller complaints can be connected to other cases. We know that many police departments and prosecutors don't have the resources to investigate and prosecute every single $500 or $1,000 loss, so we hope to be able to package cases that can be investigated together. This will reduce the chances that multiple agencies run separate investigations into the same perpetrator. And it will give police and prosecutors the full picture of what an individual perpetrator is responsible for.

IC3 was formed because the FBI believes that all cyber complaints need to be collected in a single location. Once they are collected and connected with related cases, they need to be sent back out to the agencies best suited to investigate or prosecute them.

So when an agency receives a single complaint for a $500 or $1,000 loss, we'd first like you to make sure that victim files with the IC3. The IC3 can then connect it to any related cases and get information back into the hands of the local cyber task forces, which will soon be staffed with personnel from Operation Wellspring, which I'll discuss in a minute. [See page 22.] Those task forces can then address these issues appropriately.

FBI Supervisory Special Agent Herbert Stapleton

FBI Assistant Director Joe Demarest:

People Don't Know Where to Report Cybercrime

Our goal is for IC3 to be a well-known, centralized location where these crimes can be reported. Right now people don't know where to go to report these crimes, and we estimate that only about 10 percent of all incidents are reported to us.

We see this as a good resource for all of you, because we may be able to make connections between cases and save you time from having to initiate separate investigations into crimes committed by the same offender.

FBI Supervisory Special Agent Herb Stapleton:

We Would Like Local Police To Help Spread Our Message

IC3 is just beginning its outreach efforts to local agencies. Participating in PERF's conference today is one of our first steps in doing that, so we hope that you all bring this information back to your department and share it with other agencies so that everyone knows that IC3 will be the central repository for Internet crime complaints in the United States.

continued on page 22

continued from page 21

I want to make sure that if there's only one thing you take away from our involvement in today's meeting, it's that you have www.IC3.gov written down. That's the address of the public-facing portal for filing complaints with the IC3. IC3 is designed to be a consumer reporting portal. All a victim has to do to report their crime is log on to that website, click "File a Complaint" and begin filling out their information. A law enforcement officer could do that as well, but we have other avenues within our cyber division for state and local agencies to report their cybercrime complaints.

The other benefit of IC3 is that it's one of the world's biggest collections of information about cybercrime and internet fraud trends. We try to tease out trends from the data, so we know what's coming over the horizon and can proactively warn the public about what they should be on the lookout for.

Operation Wellspring

Operation Wellspring is the approach developed by IC3 to collaborate with local law enforcement on cybercrime investigations. Pilot programs are under way with the Utah Department of Public Safety and the Dallas Police Department.[16]

FBI Assistant Director Joe Demarest:

IC3 Is Piloting Operation Wellspring With the Utah Department of Safety

IC3 has established its effectiveness at aggregating cyber complaints, and now we would like to focus on sharing that information with local agencies. We've created a pilot program with the Utah Department of Public Safety to package information that may be useful to the department. These will be cases in which the perpetrators or victims are believed to reside in the state of Utah. The Department of Public Safety has provided us with several investigators who work with our investigators to identify actionable information and get it to the appropriate people on the ground. Those state investigators came to IC3 for a two-week training, then joined our team in Utah to start working on developing case packages.

When we enter into a partnership with an organization, we will provide training and give their employees access to our operations, then work with them to address their local issues. We are also able to connect departments with other agencies that are confronting similar cybercrime challenges. **If this partnership would be useful to your agency, we are looking for more pilot sites for Operation Wellspring.**

16. New Internet Crime Initiative. *FBI News,* 24 September 2013. http://www.fbi.gov/news/stories/2013/september/new-internet-crime-initiative-combines-resources-expertise.

continued from page 19

Dallas Detective Mike Martin:

We Assist Other Agencies Whenever Possible

We have two officers assigned to the Regional Computer Forensics Lab (RCFL) in Dallas and one officer assigned 1–2 days per week at the Secret Service lab. The RCFL handles most of our forensics but some are processed at the USSS lab. We investigate all types of Internet fraud, intrusions, and cyberbullying. Part of our standard operating procedure is to assist other agencies who call us for help with cybercrime investigations.

We know it's a challenge for everyone to gather the necessary resources, so we're trying to help when we can. We generally try to point other agencies in the right direction, but we can't handle all their cases ourselves. We can't even handle all of our own cybercrime cases ourselves.

San Diego County Lieutenant Kenneth Nelson:

IC3 Helps Us Connect the Dots And Find High-Volume Offenders

I agree with everything that's been said here, but we also need to talk about intelligence sharing. The average cybercriminal is not committing one crime; they're often committing thousands of crimes. As long as there is a good platform for intelligence sharing, like IC3, we can connect the dots and put the appropriate resources into stopping the criminals who are committing thousands of crimes.

San Diego Acting Assistant Chief Lori Luhnow:

San Diego Uses Many Task Forces

We are part of four different task forces, which enable us to tackle cybercrime problems from multiple angles. We rely heavily on the Secret Service and FBI for training. We have a Regional Fraud Task Force that focuses on fraud and cases that cross jurisdictional boundaries.

San Diego Acting Assistant Chief Lori Luhnow

There is a Computer and Technology Crime High-Tech Response Team (CATCH), which is grant funded through the state of California. It is sponsored by and housed in our district attorney's office. They focus on identity theft, hacking, network intrusion, social networking, access device frauds, and wire frauds.

We also have our ICAC (Internet Crimes Against Children) unit that has 50 affiliates. There is also a Regional Computer Forensics Lab (RCFL) staffed by officers trained by the FBI to handle federal crimes.

I think having a collaborative culture has made us very successful in San Diego, and by managing these crimes through task forces, we put ourselves in the best position to handle cybercrime.

Topeka Chief Ron Miller:

Law Enforcement Will Catch Up and Respond

We are part of the Regional Computer Forensics Lab (RCFL), and we just opened a satellite lab in Topeka that is part of the RCFL out of Kansas City. We have people on the Secret Service Financial Crimes Task Force.

This is an emerging, adaptable enemy, but I

TOP: Topeka Chief Ronald Miller
MIDDLE: ICE Assistant Director Harold Hurtt
BOTTOM: Principal Deputy Assistant Attorney General Mary Lou Leary

think law enforcement will respond. We have a good opportunity here to develop the necessary collaboration to keep doing what we do best, which is to protect this country and its citizens.

Assistant Director Harold Hurtt
Immigration and Customs Enforcement:

We Need to Learn from the Private Sector

In most of these cases, the criminal isn't someone down the street or a gang member who is familiar to local law enforcement. It's often someone thousands of miles away. I think it's essential to turn to task forces to investigate these cases. Local and state agencies need the assistance of federal agencies to solve these crimes.

It's also important for all of us to work with the private sector, and I'm glad to see so many private sector representatives at this meeting today. They have already made the necessary investments to combat these crimes, and they realize the harm that can occur. The partnership between law enforcement and the private sector is stronger today than it has been in the past, and we need to utilize that partnership in what we do.

Mary Lou Leary, Principal Deputy
Assistant Attorney General,
Office of Justice Programs:

FBI and Other Federal Agencies Can Provide International Connections

Cybercrime has been a big priority for the Department of Justice, and we have assigned attorneys to work with the FBI and agencies all over the county to address cybercrime. When crimes occur that involve perpetrators from other countries, it's important to work with the FBI and other federal agencies with international connections, because we need to connect those cases.

President and CEO Maria Vello, National Cyber-Forensics & Training Alliance:

IC3 Gathers the Information To Connect Cases

Cybercrime perpetrators know no boundaries. They operate across industries and across sectors. We need to report everything so that we can put everything together, build a bigger case when one exists, and figure out how we can go after these people. IC3 provides that centralized information hub that enables collaboration.

FBI Assistant Director Joe Demarest:

The U.S. Does Coordinate With Foreign and Domestic Partners

There is a lot of coordination that the U.S. intelligence community can do with both foreign and domestic partners. Although a cyber threat to the United States may not directly impact a country in Europe, the cyber threats we face continue to evolve. We face global threats, and we must confront these challenges as a global law enforcement community.

Cooperation with Internet Service Providers and Private Corporations

Corporations are often reluctant to seem too engaged with law enforcement, citing concerns about consumer confidence in the privacy of their information. But Summit attendees reported that cooperation with some private companies is improving and those relationships can be very useful.

FBI Assistant Director Joe Demarest:

We Hope for Legislation That Would Require Internet Providers to Share Information

We don't expect legislation requiring internet service providers (ISPs) to share information with law enforcement to pass this year, but we will keep pushing for it. One issue is that the "public conversation" about privacy issues impacts Internet companies, and a company might lose business if they're seen as working too closely with the government.

We are working hard to dismantle these threats and charge those criminals who are responsible. These operations are times when we get into a delicate dance with the private sector. We can't have them do things that are inherently governmental, and we can't have their employees acting as FBI analysts, but there are things they can do, and that's a line we try to balance.

Mountain View, CA Chief Scott Vermeer:

Companies Often Don't Want To Be Seen as Pro-Government

As Mr. Demarest from the FBI mentioned, companies may not want to be viewed as pro-government. People use these companies' services because they trust that their data will be secure. But I think the private sector does want to be involved in this conversation. There are people employed in Silicon Valley who understand the law enforcement perspective.

Social media websites have become more and more cooperative with law enforcement. At first it was like pulling teeth, and even today we get some

Mountain View, CA Chief Scott Vermeer

Los Angeles Co. Chief David Betkey

resistance. Unfortunately, the interests of social media companies often just are not the same as our interests.

Toronto Deputy Chief Peter Sloly:

Many Companies Have More Cybercrime Experience Than We Do

The bad guys are already ten steps ahead of us, so we need to do some work to get caught up. In Toronto, we have partnerships going with private companies that have much more experience and expertise with cyber, social and digital than we do. These public-private partnerships (P3) are giving us guidance about how criminals are operating.

Partnerships with Universities

Los Angeles County Chief David Betkey:

We Partnered with a University On Our Crime Lab

We partnered with the LAPD and Cal State-Los Angeles a few years ago to build our crime lab. The LAPD, the Los Angeles Sheriff's Department, and the university all govern the crime lab, and it's been a very successful partnership.

Los Angeles Co. Chief William McSweeney

Los Angeles County Chief William McSweeney:

USC May Be the First University To Offer a Computer Science Forensics Degree

We asked the University of Southern California if they could open a program within their computer science department geared at forensic training. They have been very receptive, and I think they see this as an opportunity to be out in front of this issue. We haven't yet put all the pieces together, but I think USC will probably be the first school to offer this kind of degree.

We need to figure out how we will use these graduates. Will they supplant cops? Will they work with cops? Or do we hire cops and then push them in that direction? That hasn't all been worked out, but it's great to be developing this relationship.

Springfield, MO Chief Paul Williams:

We Partnered with a University On An Internship Program

When I was developing our cybercrime unit, we needed space so I went to our local college, Missouri State University, and asked if we could offer some internships in exchange for housing on campus. We worked out a deal where the university gives us free space and we give two internships a year to the computer science or criminal justice department. Those students get experience doing what they want to do, they provide some workload assistance, and it has potential as a recruiting tool.

Personnel Development

Police departments are having a difficult time hiring, training, and retaining employees who are capable of handling cybercrime investigations. Technology professionals can generally earn higher salaries in the private sector, so they are difficult to recruit. Most police officers did not enter the profession because of an interest in or aptitude for technology, so not all officers are well-suited for these positions. Once a department does identify officers for training, training programs and qualified trainers must be found. And officers who become talented at handling cybercrime may be courted by private sector companies offering higher salaries.

Agencies are also facing a fundamental question about their approach to cybercrime: Will cybercrime be delegated to a small unit within an agency, or should all officers receive cybercrime training? Departments would like all their officers to be able to handle the increasing number of complaints with a cyber component, but this is completely foreign territory for many officers.

Participants at PERF's Summit offered their perspectives on these challenges.

IDENTIFYING TALENTED PERSONNEL

Toronto Deputy Chief Peter Sloly:

You May Have Cyber Experts Already Working in Your Agency

We are trying to train our officers internally, but that isn't going to be enough to handle all the cybercrime. We need to recruit and hire people who know how to deal with this. We need an HR strategy for IT—police agencies need to hire "that millennial with a nose ring."

In Toronto, we found a 23-year-old civilian in our parking enforcement unit who knew all about computers and cyber/social/digital issues. He has been involved in solving some of our most high-profile cases, and today he represents Chief Bill Blair and the Toronto Police Service nationally and internationally, telling people about the future of cybercrime. And that was just the first person we found.

In our 7,000-person agency, I'm sure there are more employees with a similarly intuitive understanding of technology and cybercrime. These knowledgeable employees are a good place to start in building up your cyber capacity.

Toronto Deputy Chief Peter Sloly

Toronto Deputy Chief Mike Federico

Toronto Deputy Chief Mike Federico:

Track the Unique Talents Of Your Employees

One of our HR strategies is to catalogue all the talents that our recruits bring to the organization. When they graduate from the police academy, we take a close look at their background information. I would recommend that all departments keep an eye out for talented people in their graduating classes. Mine your employee data a bit more to know more about your younger members, because they may have capabilities you can capitalize on later.

We realize that it may be a challenge to keep some of these talented people in our departments when they get job offers in the private sector. We offer an employee enrichment program, but we know we can't compete with private-sector salaries. What we try to do is create an exciting environment backed with a lot of employer-provided benefits, including a pension.

We know that millennials tend to change careers frequently—every five years or so. If your organization offers opportunities for a variety of work experience, that is one way to offer them the job variety they seek and so keep them interested in staying with you.

However, it's been my experience that like us when we joined, the younger generation of police applicants is still looking for some degree of certainty for their future, and a good pension plan can really be a good recruiting tool.

Toronto Deputy Chief Peter Sloly:

Employees May Go to Private Sector But Come Back to Policing Later

We know that we may not be able to keep really talented cyber/social/digital experts in our department forever. In my mind, the goal really shouldn't be to keep these people for 25 years. If you keep them more than five years, their knowledge and expertise will become stale, so their value may actually start to trail off.

So I think you can encourage your experts to leave for the private sector. Five years later, when they have made some money and learned some new skills, they may want to come back and work for the police again. The bottom line is that police agencies need a new HR strategy for IT.

Executive Director Michael Kaiser, National Cyber Security Alliance

Executive Director Michael Kaiser, National Cyber Security Alliance:

High School and College Cyber Competitions Showcase Talented Young People

Developing a talent pool capable of doing these technology jobs is an important issue for local law enforcement agencies and the federal government. There are high school and college-level cyber teams and competitions across the country to showcase students' technological abilities. Law enforcement should be part of that.

When I went to the Maryland Cyber-Challenge in October, there were many private-sector representatives recruiting the talent. They were offering internships, jobs, and scholarships. Police agencies should participate and offer what we can.

In many cases there are already police officers in these schools. School Resource Officers may be able to help recruit talented people from within your community.

Detective Chief Superintendent Paul Rumney, Greater Manchester Police:

We Use Seized Funds To Hire More Investigators

We have very strong powers under the Proceeds of Crime Act, so even if we can't catch the perpetrators, we will probably try to chase the money, because it can be seized. Once we seize it, we invest it back into proactive operations.

In Greater Manchester, we have 12 full-time financial investigators, and their salaries are funded by the money that was seized under the Proceeds of Crime Act. This has let us invest in a number of specialists who deal with financial crimes that victimize members of the public.

Chief Terrance Gainer, U.S. Senate Sergeant at Arms:

We Should Train Our Employees On Safe Use of Technology

With all the electronics we use in our offices, we need to educate our employees about how they should protect themselves. Our system counts 100 instances a day of people in the Senate community trying to access websites that we consider malicious. I think we need to educate our employees to make sure they aren't unintentionally making us vulnerable through unsafe Internet use.

This might be necessary especially for those of us who didn't grow up with these technologies. I'm sure most people in this room have had to ask their administrative assistant or a younger person in their office to fix a technology problem we can't resolve. I think many of us could use a training program ourselves to make sure we're using technology safely.

Because we all use technology so often, I think we need to be careful not to just train specialists to deal with technology issues. All our employees need an understanding of technology and how it can help or hurt them and the organization. We are better off when our employees are well-rounded.

Chief Terry Gainer,
U.S. Senate Sergeant at Arms

United States Secret Service
Special Agent in Charge Ed Lowery

CYBERCRIME TRAINING

Detective Chief Superintendent Paul Rumney, Greater Manchester Police, UK:

Our Greatest Challenge Is Finding Trainers

Training is the greatest challenge for us at a local level. We bring in specialists from banking institutions. We also use the National Crime Agency to teach about prevention activity, particularly about emerging threats and issues like vulnerability and cyber bullying. But this issue is still is very much in its infancy at a local level.

Special Agent in Charge Ed Lowery, U.S. Secret Service:

The Secret Service Has Provided Training To More than 3,000 State and Local Officers

About ten years ago, the Secret Service realized that our investigations required our agents to know how to collect evidence from a mobile device or a social networking site. We started teaching investigators the basics of cyber investigations, which improved the situation. As a result of our collaborative work with other law enforcement agencies, we also recognized that state and local departments shared this issue, and that smaller agencies don't always have access to high-tech labs.

In 2007 we began working with the state of Alabama to provide training at the National Computer Forensics Institute (NCFI) in Hoover, Alabama. At NCFI, we bring in investigators from agencies across the United States and provide them with the same training that we give to our agents.

Depending on the needs of the individual agencies, we can provide specialized trainings in areas including cyber forensics, network intrusion, or mobile devices. Officers are nominated through their local Secret Service office, and all NCFI housing, travel, per diem, and equipment is provided by the program. These officers return to their department fully prepared to conduct cyber investigations.

To date, we have trained over 3,000 state and local officers since the program began in late 2008. We've also started including prosecutors and judges after some of our graduating officers told us that they were presenting the results of their cyber investigations to prosecutors and judges who didn't understand what they were seeing.

Tim Murphy, MacAndrews and Forbes Vice President and former FBI Deputy Director:

Cyber Investigations Are Not as Daunting as We May Think

I think we make some of this more complicated than it actually is. You don't need to know every last thing about how the Internet works to be a good cyber-investigator. Many cases will be investigated very similarly, so you just need to know what useful investigative information you can obtain, like IP addresses, and then how to make that information work for you. You may do this by relying on some expertise inside or outside your organization. Cyber expertise is just another tool that can improve our

investigative capabilities. However, the general investigation steps to solving problems remain the same.

Madison, WI Lieutenant June Groehler:

We Are Working on State Certifications For Cybercrime

We have all the usual state-required certifications and re-certifications for our officers, but we don't have any requirements for cybercrime. So I reached out to the Wisconsin Law Enforcement Standards Board to point this out, and today subject matter experts with real-world experience are creating curriculum to address high-tech crimes and technology. This will allow us to teach and develop our future law enforcement officers and bring everyone in our department up to speed, since the use of technology has become ubiquitous in modern society.

Detective Chief Superintendent Paul Rumney, Greater Manchester, UK Police:

Different Officers Need Different Levels of Training

Our approach to cybercrime training needs to have several tiers. You cannot reasonably expect a local front-line police officer to deal with a complex cybercrime syndicate from an Eastern European country that is targeting large institutions or public infrastructure.

But the public does have the expectation that our officers will be able to handle some common situations. For example, if parents contact the police service to report that their child has been bullied online, the police service has to show some degree of competency and capability when addressing these issues, in order to maintain credibility in the community.

DOJ Bureau of Justice Assistance Director Denise O'Donnell:

The National White Collar Crime Center Offers Training

The National White Collar Crime Center is a good resource for economic crime and cyber training. They go into law enforcement agencies and prosecutors' offices and conduct on-site training that can really improve your cybercrime investigations.

Detective Chief Superintendent Paul Rumney, Greater Manchester Police:

All UK Agencies Are Building Cybercrime Capabilities

We are having the same conversations in the UK about cybercrime, including discussions of jurisdiction and the need for specialists versus improving the capabilities of front-line police. We have the National Crime Agency, the Serious and Organized Crime Agency, and the Regional Organized Crime Units, which all have expertise we can draw upon. But the Home Office still has the expectation that all police forces in the UK will have some kind of cybercrime capability. So we're training all the individual agencies. I think the larger, better-funded forces are gaining cybercrime capabilities faster than the smaller forces.

Principal Deputy Director Josh Ederheimer, DOJ COPS Office:

Police Response Starts With Responding Patrol Officers, So They Need to Understand The Basics of Cybercrime

The confidence and trust a community has for their police department is an important measure of effectiveness for an agency. When an iPhone is stolen, the owner can use an app to locate it. If the victim tries to explain this to the responding officer and gets a blank stare, that crime victim isn't going to have a lot of confidence in the police.

I hear a lot about specialized units, and they will

Principal Deputy Director
Josh Ederheimer, COPS Office

certainly be important for intelligence gathering. But it really is going to start with the patrol officers who are the first ones to answer the call. They need to know how to collect the right information and ask the right questions, so it can be passed along to the next level.

San Diego Acting Assistant Chief Lori Luhnow:

When Patrol Officers Know the Basics, They Can Step Up to a Cyber Division

We have seen value in training all our officers in cybercrime, specifically patrol officers who benefit by having the appropriate tools in the field to initiate investigations. We are seeing a certain degree of burnout from people specializing in our cybercrime units, and their desire to move on after a few years. It's been good to have others already trained in the basics and waiting in the wings to assist.

Director William O'Toole, Northern Virginia Criminal Justice Training Academy:

Officers Apply Existing Skills to Cybercrimes

We believe that all officers need to have some basic understanding and skills related to cybercrime investigations. They should know how to recognize electronic evidence and be able to flag and secure things for follow-up by those with more expertise.

Our academy relies on the National White Collar Crime Center and on specially trained investigators from our larger agencies to provide training on the seizure of electronic evidence. We want our patrol officers to use the same skills of observation, awareness, and good documentation that they use for all crimes and apply them to cybercrime.

RIGHT:
Director William O'Toole, Northern Virginia Criminal Justice Training Academy
FAR RIGHT:
Co-Founder Ron Plesco, National Cyber-Forensics and Training Alliance

FBI Supervisory Special Agent Jacques Battiste

POLICE EXECUTIVE FELLOWSHIP PROGRAM

The Police Executive Fellowship Program is a six-week program that brings law enforcement executives to FBI headquarters to work in areas that will improve law enforcement information sharing.[17] *Some fellows are assigned to the FBI's Cyber Division, and several participants at PERF's Summit had been involved with the program.*

FBI Assistant Director Joe Demarest:

Our Fellowship Program Teaches Cyber Skills

Our Police Executive Fellowship Program brings people in from state and local agencies across the country. During their six months at the National Cyber Joint Investigative Task Force, they have the opportunity to see every aspect of the task force's operations. When the fellows go back to their individual agencies, they can share what they've learned with others. We know that no one agency can do everything by itself, so we'd like to expose more agencies to what we're doing.

San Diego County Lieutenant Kenneth Nelson:

The Fellowship Program Was a Valuable Experience

I was fortunate to be assigned to the National Cyber Investigative Joint Task Force while participating in the FBI's Police Executive Fellowship Program. I had more background in criminal investigations and fraud than in cybercrime when I joined the task force. Seeing the information the task force coordinates between various federal, state, and local agencies was eye-opening. I was very impressed by the resources and training that is available from federal agencies.

FBI Supervisory Special Agent Jacques Battiste:

Our Fellows Also Teach Us

Our fellowship program isn't only about us training the fellows. Many of the people who take part in the program come with their own wealth of knowledge from the state and local level. We learn about the capabilities and needs of the local and state agencies, and they learn from each other.

Police Department Network Security

Many police departments' websites have been hacked, including a February 2012 intrusion in which the Boston Police Department's website was taken offline. A few days later, the Dallas Police Department's website was hacked and officer data was stolen.[18]

17. "Police Executive Fellowship Program." Federal Bureau of Investigation. http://www.fbi.gov/about-us/office-of-law-enforcement-coordination/pefp.
18. Dallas Police Department's Website Hacked. *NBC Dallas-Fort Worth,* 7 Feb 2012. http://www.nbcdfw.com/news/tech/Dallas-Police-Departments-Website-Hacked-138823209.html.

Police agencies are entrusted with the personal information of both their communities and their officers, so network security is essential to ensure that that trust is not violated.

San Diego County Lieutenant Kenneth Nelson:

We Need to Secure the Sensitive Information On Our Network

All law enforcement agencies should make network security a priority. My department is a paperless department, so the information stored on our networks encompasses victim and witness data, investigative notes, crime and arrest reports, personnel information and other sensitive data. A breach of the system and the loss of this data could be extremely harmful. Every agency could do a better job of securing their data. The threat is constantly evolving and changing.

Tim Murphy, MacAndrews and Forbes Vice President and former FBI Deputy Director:

Hacking Incidents Can Erode Community Confidence

The first step is to secure your own network. You need to ask yourself if you're more safe from a cyber-attack today than you were yesterday. If the answer is no, or you don't know, then you need to do something about it. If we don't secure our own systems, we lose the confidence of the community. If criminals start defacing your website, breaching your systems and obtaining your data, the community is going to lose faith in your ability to protect them in the cyber world and the real world.

Philadelphia Commissioner Charles Ramsey:

Cybersecurity Often Isn't a Funding Priority

In my department, as with most departments, funding is always an issue. This means elected leaders need to decide on priorities, but until there is a major incident, it's difficult to have the kind of IT budget necessary to develop a strong cybercrime program and protect our own systems.

We need to get this on the minds of the right people so that we can develop systems to get a reasonable level of protection. I don't think anything we develop will be totally foolproof, because I'm sure someone extremely technologically-savvy could penetrate anything we develop. But with some funding we can probably install a system that would prevent small-time hackers from getting in. We are also concerned about whether we have anyone internally with the level of expertise to put together a sufficient protection system.

So I'd say it's a huge concern for us, but it's not one that I think is going to be resolved soon for funding and personnel reasons.

Community Education

Chief Superintendent Stephen Cullen, New South Wales, Australia Police Force:

We Must Educate the Public About Cyber Dangers, Especially Those Who Are Less Skilled with Computers

Our community engagement is not sufficient. In particular, the elderly in our country have been

San Diego County Lieutenant Kenneth Nelson

Philadelphia Commissioner
Charles Ramsey

targeted because they tend to be less skilled with computers. They will respond to emails that they should not open and fall victim to crimes. We are just starting to fulfill our responsibility to get out in front of that with education programs.

Madison Lieutenant June Groehler:

We've Developed A Strong Community Education Program

The Madison Police Department posts cyber-safety tips and a list of online resources on its website at https://www.cityofmadison.com/police/safety/cyber/.

While police departments across the country now investigate the explosive rise of cybercrime and address related digital media activities, the Madison Police Department has gone further and created a multi-disciplinary, community-based approach to promote greater understanding and knowledge about cybercrime and safe use of digital media.

In early 2009, the Madison Police Department started to realize the impact that cybercrime and the increasing use of digital media were having on our community. Increasingly, parents were contacting MPD for information on cybercrime. A number of cybercrime-related incidents had taken place in our community. One incident evolved into a multi-jurisdictional investigation and arrest of a 22-year-old Gloucester, Mass. man who traveled to Madison in an attempt to kidnap and harm a 17-year-old he had met online playing the popular Internet game "World of Warcraft."

Our initial approach was simple: disseminate information on cyber safety to community members through evening meetings at district stations. The first meetings had large numbers of attendees and attracted interest from local news media. Topics included basic cyber safety when using social networking sites, cyber bullying, general Internet safety, online gaming, and the use of cell phones. Many in attendance, particularly parents, told officers how the presentation made them realize how little they knew about the dangers that come with new technologies.

By early 2010, it was becoming increasingly apparent that a more comprehensive approach was

New South Wales, Australia
Chief Superintendent Stephen Cullen

necessary. Cyber safety presentations were important, but other strategies were necessary, so we took several more steps:

- A DVD was created covering information from the community cyber safety classes. The DVD includes interviews with victims of cyber crimes. The DVD was mass-produced and over 5,000 have been sent out to law enforcement agencies and families not only in Wisconsin, but also throughout the United States.
- A group of MPD officers formed a Technology Committee in response to requests from the community. These officers created a curriculum on cyber safety for classroom environments equipped with computers. Each participant received the opportunity to use various social media applications and learn in more depth about Internet use and safety.
- These same officers created a Youth Cyber Detective Camp. In another "hands on" approach, youth worked through case studies of cyber bullying cases and teen suicides. And the students teach us about the new technology they face day to day. We recently were taught about the new wave of hot apps such as Kik, WhatsApp, and Snapchat.
- In early 2011, the Madison Area Council on Cyber Safety for Children was created. In partnership with the Madison Police Department, several local businesses, health groups and schools have committed funds, time and staff to further develop and expand MPD's cyber safety initiatives.

Police departments conducting presentations on cyber safety are certainly not novel. However, the Madison Police Department cyber safety initiative

Madison Police Department's Cyber Camp Shows Youths How to Avoid Being Victimized

The Madison, Wisconsin Police Department holds an annual week-long cyber detective camp for middle school students called "Middle School U." Students are given a mock case report involving a cybercrime, and spend the week investigating and solving the case.

The cases are fictional but are based on components of actual cases the Madison Police Department has investigated. For example, the 2013 camp involved a fictional 8th-grade girl who failed to come home one day. The Cyber Camp participants "interviewed" the missing girl's parents and friends (who were Police Department interns serving as actors). The interview process revealed that the missing girl had created a fake Facebook account, unknown to her parents, and used it to meet a man who was in his 20s but had presented himself to the missing girl as a high-school student.

Thus, during the camp, students learn about cyber safety issues that could affect them. They also learn about the Madison Police Department and police work in general. Various elements of policing are included, such as interviewing skills, use of K-9s (to find the missing girl's backpack), handling of electronic evidence (the missing girl's computer), and so on.

The Middle School U camp began in 2010 and was considered a success, leading to the development of a similar camp for high school students in 2011 that continues today.

has gone well beyond this and evolved into a community-wide partnership and collaboration. The Madison Area Council on Cyber Safety for Children includes local businesses (e.g. Johnson Bank, Epic Systems, In Business Magazine), health organizations (University of Wisconsin Hospitals and Clinics, Group Health Cooperatives), and local school districts. It is this multi-disciplinary partnership of diverse organizations that have joined together with MPD to create a multitude of approaches to addressing the topic of cyber safety.

The large numbers of adults and youths who seek to attend our cyber safety classes attest to our effectiveness. We also continue to receive many requests from law enforcement agencies throughout Wisconsin and across the United States for information on our multi-disciplinary approach. In these early years of building greater awareness and understanding of cybercrime, we believe we are starting to see increased reporting to MPD of cyber crime incidents, particularly cyber bullying.

The tragedies we see each day, particularly with our youth, bring to the forefront the significance of cyber safety in the world we live in today. For the first time, we have a generation of youth who will grow into adulthood and be known as the first "digital generation." The means by which they communicate, are educated, work and play will be by emerging and evolving digital technologies. We already have seen instances of cyber crime once thought to be unimaginable. As we saw firsthand in Madison, who would have ever thought, ten years ago, that a 22-year old from Massachusetts, addicted to an online computer game, would travel by car 1,100 miles to kidnap and likely kill an online adversary? So while new technologies often make our lives more enjoyable, they have also created new realities that all communities must face.

Every aspect of our program is transferable to other communities and law enforcement agencies. We share our curricula with anyone who asks, and provide consultation to law enforcement agencies that want to start a cyber safety program. Our next phase includes an updated DVD with an interactive media component that will be made into an "App," designed to reach a national audience through digital dissemination.

What is possibly unique in Madison is the desire we see by many different organizations, across different disciplines, to partner with us in our cyber safety education efforts. In the near future, you will see our "App" for a compelling game that blends learning goals into the game play. This will certainly be a milestone for us, and nothing we foresaw a few years ago when a handful of officers decided to give presentations to the community on cyber safety. As new technologies evolve, so too must our cyber safety educational efforts.

Use of Social Media For Investigation and Crime Prevention

WHILE CYBERCRIME IS DEFINED AS CRIMES *facilitated by the use of computers or the Internet, there is a related "flip side" of the issue: police departments' use of computers and the Internet to investigate crimes. In particular, participants at PERF's Summit discussed how they are using social media for intelligence and investigations.*

In Northern California, for example, several agencies assign gang investigators to scan social media for signs of gang activity. Santa Clara County Deputy District Attorney Lance Daugherty estimates that over 25 percent of gang felony cases include evidence from social media, and Contra Costa County District Attorney Tom Kensok estimates that more than 50 percent of gang cases include evidence from social media.[19] *This evidence comes from a variety of sites, including Twitter, Facebook, Instagram, and YouTube.*

Director Daphne Levenson, Gulf States Regional Center for Public Safety Innovations

Director Daphne Levenson, Gulf States Regional Center for Public Safety Innovations:

Using Social Media Can Save Time

We've found that departments with a proactive social media strategy see a good return on their investment. There are crimes that they solve in five minutes that previously would have required days of investigation, because the community is involved and provides information that police wouldn't have had before. The entire city becomes involved in the police department. Social media can be a valuable resource for the community to tell you what is going on.

On the preventive side, you can educate your community by sending out warnings about scams through social media. These preventive and investigative measures free up staff to deal with other issues. It's a smart use of funding and improves your community involvement.

19. Cyberspace emerges as law enforcement's new battleground. *Contra Costa Times,* February 21, 2014. http://www.contracostatimes.com/news/ci_25204778/cyberspace-emerges-law-enforcements-new-battleground

Newark Police Director Samuel DeMaio:

Investigators Assigned to Social Media Are an Investment That Pays Off

We have a lieutenant in our intelligence unit who is always looking at social media to let us know where the next crime is going to occur and how we might be able to stop it. I'd like to expand this program so we can do a better job with it. Our city sees a lot of violence, and I think we need more people to investigate these cases on social media. I think it's an investment that would pay off.

Toronto Deputy Chief Mike Federico:

Be Aware of the Latest Innovations

Cyber-preparedness is a combination of investment in human resources and investment in technology. To the latter point, we need to be aware of the latest technological innovations. We found open-source freeware that can insert people into online activities that may appear private but are actually public, like Facebook and Twitter. The combination of these investments can really advance the policing profession.

Geo-Fencing

Geo-fencing is a technology that narrows searches for information in the virtual world. Police can search social media to only include posts that occurred near a certain event—for example, Facebook posts or tweets that were made shortly after a crime was committed, by people who were near the crime scene when they posted their comments online.

Toronto Deputy Chief Peter Sloly:

Geo-Fencing Gives Us More Information Than We Could Get with 30 Officers Scouring a Crime Scene

Geo-fencing has been an important tool for us. For those who don't know, geo-fencing is a way to search for open-source social media content within defined geographical areas and time frames. You can put up a geo-fence anywhere. We usually do it down to a specific postal code, but you could apply it to narrower parameters if that would be more effective.

We had a stabbing occur during a large festival this past summer. We ran a geo-fence around the street and several surrounding streets, and we picked up thousands of Facebook and Twitter posts that occurred within minutes of that incident. It gave us a huge source of witnesses.

We were also able to look at photos posted on social media around the time of the incident. And we used social media to piece together any gang associations that may have had a role in the stabbing. We have another software tool that can catalogue all of a person's associations from a single tweet or Twitter account. We got more information from that than we would have from having 30 officers canvass the area of the scene for three days. We were also able to keep an eye on social media for possible revenge crimes and know the hot spots where those might occur.

Do these cyber/social/digital tactics prevent or

Arlington TX Assistant Chief Lauretta Hill

solve every crime? No, but it allows police to leverage technology across all core operations, and it produces a lot of rich information and useful data.

Arlington, TX Assistant Chief Lauretta Hill:

Geo-Fencing Helped Us During the Super Bowl

We have a tactical intelligence unit that uses software called Snap Trends that has geo-fencing and other social media tracking and linking capabilities, to look at all the social media feeds from within a specific area. During the Super Bowl, we worked with the FBI to look at what people were talking about online. At a practice exercise prior to the Super Bowl, someone sent a tweet saying there was a bomb at the stadium. We were able to immediately determine the person's exact location in Louisiana and could send the FBI to his house right away. Using this tool gives us more information about what's occurring.

Conclusion

WHILE PERF HAS PRESENTED A NUMBER OF promising practices in this report, it is clear that local police agencies are still in the early stages of developing comprehensive strategies for responding to and preventing cybercrime. Additional work needs to be done to ensure that every police officer will know how to respond to a cybercrime call; detectives will understand the avenues that are available for investigating these crimes; and local, state, and federal authorities will have an effective system for sharing information, connecting cases committed by the same offenders, and coordinating investigations.

Our Summit participants recommended several steps that police departments can take to respond to cybercrime. Those steps include:

- **Participating in task forces.** Task forces use the resources of local, state, and federal agencies to investigate cases that would be too large or complex for one agency to handle alone. Electronic Crime Task Forces (ECTFs), managed by the U.S. Secret Service, and Regional Computer Forensics Labs (RCFLs), created by the FBI, provide federal assistance on a regional basis.

- **Working with private corporations.** In many cases, private corporations have more experience with cybercrime investigations than local police agencies. Corporate officials often have a great deal of respect for their local police officials and are glad to build these partnerships.

- **Working with local universities.** A number of police agencies have formed partnerships with computer science departments at local universities. These partnerships not only provide expertise to the police, but also serve as a recruiting tool for students who have an interest in cybercrime and policing.

- **Identifying, recruiting, and training talented personnel.** Police departments need employees who are capable of handling cybercrime issues. Some police departments are undertaking a variety of strategies for identifying and recruiting potential employees with knowledge of information technologies, and identifying current police employees who have an interest in cyber issues and can be trained to play an important role in the department's cybercrime prevention and investigation efforts.

  The U.S. Secret Service has trained more than 3,000 state and local law enforcement officials in cybercrime forensics and related topics. The FBI offers the Police Executive Fellowship Program, a six-month program about information sharing that includes cybercrime education. And the National White Collar Crime Center also offers training to local police and prosecutors' offices.

- **Educating the community.** Many cybercrimes are preventable by taking appropriate security measures while using electronic devices. To protect community members from becoming victims

of cybercrime, police departments should have education programs to teach people about common cyber-threats and the basics about how they can stay safe online.

- **Utilizing the Internet Crime Complaint Center (IC3).** Several participants at PERF's Summit emphasized the importance of the Internet Crime Complaint Center. IC3 has been set up by the FBI to serve as a central clearinghouse for all Internet crime complaints, but the Bureau estimates that IC3 currently receives reports about approximately 10 percent of cybercrimes. To support this centralized resource and to become more familiar with cyber issues, all law enforcement agencies should encourage cybercrime victims to file complaints with IC3.

A number of police executives have noted that public confidence in the police will depend in part on whether the police can respond to and investigate cybercrime cases as effectively as they handle other types of cases. As cybercrime continues to increase in scope, members of the community will have increasing expectations that their local police will be familiar with cybercrime issues, will provide guidance on cybercrime prevention, and will be competent in investigating crimes that are committed.

Police agencies nationwide have achieved remarkable successes over the last generation; violent crime rates have declined by half since the early 1990s. But cybercrime is a new type of phenomenon that requires new solutions from local police agencies. At PERF's Summit, leading police executives delivered a wake-up call, alerting the field that law enforcement agencies at all levels must take on this new challenge.

Resources

FBI Cybercrime Homepage

Includes links to pages on Key Priorities such as identity theft and computer and network intrusions, Partnerships such as Cyber Task Forces and Cyber Action Teams, "Cases and Takedowns" highlighting major investigations, Most Wanted Cyber Offenders, Common Internet Frauds, and news media stories about cybercrime.
http://www.fbi.gov/about-us/investigate/cyber

FBI Regional Computer Forensics Laboratories

The FBI has established 16 Regional Computer Forensics Laboratories (RCFLs) across the United States. These RCFLs are full-service forensics labs and training facilities, where local law enforcement agencies can send digital evidence to be examined or have their officers trained in digital forensics.
http://www.rcfl.gov/index.cfm

FBI Police Executive Fellowship Program

The FBI Police Executive Fellowship Program brings management-level local, state, tribal, and campus law enforcement officials to FBI Headquarters for six-month fellowships. Some fellows are assigned to the Cyber Division.
http://www.fbi.gov/about-us/office-of-law-enforcement-coordination/pefp

National White Collar Crime Center

The National White Collar Crime Center (NW3C) supports state and local law enforcement with economic and computer crime through training, investigative support, and coordination. NW3C worked with the FBI to form IC3.
http://www.nw3c.org/Home

Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3) was established by the FBI and the National White Collar Crime Center to serve as the central clearinghouse for all Internet crime complaints and connect and refer cases back to law enforcement agencies as appropriate. Law enforcement agencies should encourage all cybercrime victims to file complaints with IC3 to improve nationwide data and intelligence about cybercrime.
http://www.ic3.gov/default.aspx

U.S. Secret Service

Under the USA Patriot Act of 2001, the Secret Service was mandated to establish a national network of Electronic Crimes Task Forces—panels of local, state, and federal law enforcement, as well as prosecutors, private companies, and academics.
http://www.secretservice.gov/ectf.shtml

U.S. Secret Service National Computer Forensics Institute

The National Computer Forensics Institute (NCFI) offers federally-funded training courses to state and local law enforcement, prosecutors, and judges. The course topics include current cybercrime trends, investigative methods, and challenges.
https://www.ncfi.usss.gov/ncfi/

Internet Crimes Against Children Task Force Program

This program, funded by the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention, is a national network of 61 law enforcement task forces that helps state and local agencies address online child victimization and child pornography. They provide technical help with forensics and investigations, training, victim service, and community education.
http://www.ojjdp.gov/programs/progsummary.asp?pi=3

National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) was formed by leading technology companies to educate individuals about safe online behavior and raise awareness about the importance of cybersecurity.
https://www.staysafeonline.org/

National Cyber-Forensics & Training Alliance

This non-profit connects subject matter experts in the public and private sectors to address cybercrime, particularly crimes that originate internationally. NCFTA stays up-to-date on the latest cybercrime trends and has initiatives to address some of the most common forms of cybercrime, including malware and financial crimes.
http://www.ncfta.net/Index.aspx

SEARCH

SEARCH is a non-profit membership group comprised of one gubernatorial appointee from each of the 50 U.S. states, the District of Columbia, and the U.S. territories. Through funding from the Bureau of Justice Assistance, SEARCH operates a High-Tech Crime Training program led by subject matter experts who provide training classes, workshops, and hands-on assistance to state and local agencies.
http://www.search.org/get-help/training/high-tech-crime-investigations/

About the Police Executive Research Forum

THE POLICE EXECUTIVE RESEARCH FORUM (PERF) is an independent research organization that focuses on critical issues in policing. Since its founding in 1976, PERF has identified best practices on fundamental issues such as reducing police use of force; developing community policing and problem-oriented policing; using technologies to deliver police services to the community; and developing and assessing crime reduction strategies.

PERF strives to advance professionalism in policing and to improve the delivery of police services through the exercise of strong national leadership; public debate of police and criminal justice issues; and research and policy development.

The nature of PERF's work can be seen in the titles of a sample of PERF's reports over the last decade.

- *Social Media and Tactical Considerations for Law Enforcement (2013)*
- *Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies (2013)*
- *Civil Rights Investigations of Local Police: Lessons Learned (2013)*
- *A National Survey of Eyewitness Identification Procedures in Law Enforcement Agencies (2013)*
- *An Integrated Approach to De-Escalation and Minimizing Use of Force (2012)*
- *Improving the Police Response to Sexual Assault (2012)*
- *How Are Innovations in Technology Transforming Policing? (2012)*
- *Voices from Across the Country: Local Law Enforcement Officials Discuss the Challenges of Immigration Enforcement (2012)*
- *2011 Electronic Control Weapon Guidelines (2011)*
- *Managing Major Events: Best Practices from the Field (2011)*
- *It's More Complex than You Think: A Chief's Guide to DNA (2010)*
- *Guns and Crime: Breaking New Ground By Focusing on the Local Impact (2010)*
- *Gang Violence: The Police Role in Developing Community-Wide Solutions (2010)*
- *The Stop Snitching Phenomenon: Breaking the Code of Silence (2009)*
- *Violent Crime in America: What We Know About Hot Spots Enforcement (2008)*
- *Promoting Effective Homicide Investigations (2007)*
- *"Good to Great" Policing: Application of Business Management Principles in the Public Sector (2007)*
- *Police Management of Mass Demonstrations: Identifying Issues and Successful Approaches (2006)*
- *Strategies for Intervening with Officers through Early Intervention Systems: A Guide for Front-Line Supervisors (2006)*
- *Managing a Multi-Jurisdiction Case: Identifying Lessons Learned from the Sniper Investigation (2004)*
- *Community Policing: The Past, Present and Future (2004)*
- *Racially Biased Policing: A Principled Response (2001)*

In addition to conducting research and publishing reports on our findings, PERF conducts management studies of individual law enforcement agencies; educates hundreds of police officials each

year in a three-week executive development program; and provides executive search services to governments that wish to conduct national searches for their next police chief.

All of PERF's work benefits from PERF's status as a membership organization of police officials, who share information and open their agencies to research and study. PERF members also include academics, federal government leaders, and others with an interest in policing and criminal justice.

All PERF members must have a four-year college degree and must subscribe to a set of founding principles, emphasizing the importance of research and public debate in policing, adherence to the Constitution and the highest standards of ethics and integrity, and accountability to the communities that police agencies serve.

PERF is governed by a member-elected President and Board of Directors and a Board-appointed Executive Director.

To learn more about PERF, visit www.policeforum.org.

We provide progress in policing.

About Motorola Solutions and the Motorola Solutions Foundation

MOTOROLA SOLUTIONS IS A LEADING PROVIDER of mission-critical communication products and services for enterprise and government customers. Through leading-edge innovation and communications technology, it is a global leader that enables its customers to be their best in the moments that matter.

Motorola Solutions serves both enterprise and government customers with core markets in public safety government agencies and commercial enterprises. Our leadership in these areas includes public safety communications from infrastructure to applications and devices such as radios as well as task specific mobile computing devices for enterprises. We produce advanced data capture devices such as barcode scanners and RFID (radio-frequency identification) products for business. We make professional and commercial two-way radios for a variety of markets, and we also bring unlicensed wireless broadband capabilities and wireless local area networks—or WLAN—to retail enterprises.

The Motorola Solutions Foundation is the charitable and philanthropic arm of Motorola Solutions. With employees located around the globe, Motorola Solutions seeks to benefit the communities where it operates. We achieve this by making strategic grants, forging strong community partnerships, and fostering innovation. The Motorola Solutions Foundation focuses its funding on public safety, disaster relief, employee programs and education, especially science, technology, engineering and math programming.

Motorola Solutions is a company of engineers and scientists, with employees who are eager to encourage the next generation of inventors. Hundreds of employees volunteer as robotics club mentors, science fair judges and math tutors. Our "Innovators" employee volunteer program pairs a Motorola Solutions employee with each of the nonprofits receiving Innovation Generation grants, providing ongoing support for grantees beyond simply funding their projects.

For more information on Motorola Solutions Corporate and Foundation giving, visit www.motorolasolutions.com/giving.

For more information on Motorola Solutions, visit www.motorolasolutions.com.

APPENDIX
Participants at the PERF Summit "The Role of Local Law Enforcement in Combating Cybercrime"
September 10, 2013, Washington, DC

Deputy Chief Andrew Acord
DALLAS POLICE DEPARTMENT

Chief Hassan Aden
GREENVILLE, NC POLICE DEPARTMENT

Captain Cindy Allen
AMTRAK POLICE DEPARTMENT

Inspector Robert Allen
RAMSEY COUNTY, MN SHERIFF'S OFFICE

Deputy Chief Sharon Allen
TUCSON, AZ POLICE DEPARTMENT

Sergeant Jessica Anderson
HOUSTON POLICE DEPARTMENT

Chief Michael Anderson
METROPOLITAN NASHVILLE POLICE DEPARTMENT

Commander Bradley Arleth
SPOKANE, WA POLICE DEPARTMENT

Deputy Chief Kristine Arneson
MINNEAPOLIS POLICE DEPARTMENT

Captain Michael Baumaister
TAMPA POLICE DEPARTMENT

Chief David Betkey
LOS ANGELES COUNTY SHERIFF'S DEPARTMENT

Lieutenant Bob Blakley
FAIRFAX COUNTY, VA POLICE DEPARTMENT

Corporal Joshua Brackett
PRINCE GEORGE'S COUNTY, MD POLICE DEPARTMENT

Program Specialist Melissa Bradley
COPS OFFICE (USDOJ)

Vice President for Corporate Security Brad Brekke
TARGET CORPORATION

Deputy Chief Allwyn Brown
RICHMOND, CA POLICE DEPARTMENT

Chief Chris Burbank
SALT LAKE CITY POLICE DEPARTMENT

Lieutenant Wayne Burgess
FAYETTEVILLE, NC POLICE DEPARTMENT

Chief Leonard Campanello
GLOUCESTER, MA POLICE DEPARTMENT

Commissioner Patrick Carroll
NEW ROCHELLE, NY POLICE DEPARTMENT

Assistant Chief Luiz Casanova
NEW HAVEN, CT POLICE DEPARTMENT

Chief James Cervera
VIRGINIA BEACH, VA POLICE DEPARTMENT

Assistant Chief Bradley Chandler
FAYETTEVILLE, NC POLICE DEPARTMENT

Dr. Brett Chapman
NATIONAL INSTITUTE OF JUSTICE

Captain Cory Christensen
FORT COLLINS, CO POLICE DEPARTMENT

Executive Director David Cid
MEMORIAL INSTITUTE FOR THE PREVENTION OF TERRORISM

Lieutenant Jennifer Coe
LOUISVILLE METRO POLICE DEPARTMENT

Principal Deputy John Cohen
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Chief Sheilah Coley
NEWARK, NJ POLICE DEPARTMENT

Lieutenant Todd Coyt
ATLANTA POLICE DEPARTMENT

Director Darren Cruzan
BUREAU OF INDIAN AFFAIRS

Chief Superintendent Stephen Cullen
NEW SOUTH WALES, AUSTRALIA POLICE FORCE

Retired Chief Charlie Deane
PRINCE WILLIAM COUNTY, VA POLICE DEPARTMENT

Director Samuel DeMaio
NEWARK, NJ POLICE DEPARTMENT

Assistant Director Joseph Demarest
FBI

Lieutenant William Desmond
FAIRFAX COUNTY, VA POLICE DEPARTMENT

Police ID Officer Matthew Dillon
JERSEY CITY, NJ POLICE DEPARTMENT

Chief Kim Dine
UNITED STATES CAPITOL POLICE

Ms. Maggi McLean Duncan
TENNESSEE ASSOCIATION OF CHIEFS OF POLICE

Captain James Durr
EUGENE, OR POLICE DEPARTMENT

Lieutenant Richard Duvall
ANNE ARUNDEL COUNTY, MD POLICE DEPARTMENT

Captain Todd Dykstra
DES MOINES POLICE DEPARTMENT

Acting Director Joshua Ederheimer
COPS OFFICE (USDOJ)

Senior Police Advisor Steve Edwards
BUREAU OF JUSTICE ASSISTANCE

Mahogany Eller, Public Safety Partnerships – National
TARGET CORPORATION

Titles reflect participants' positions at the time of the meeting in September 2013.

Retired Detective Joseph Ellman
DOBBS FERRY, NY POLICE DEPARTMENT

Deputy Chief Mike Federico
TORONTO POLICE SERVICE

Analyst Mora Fiedler
COPS OFFICE (USDOJ)

Commander Tony Filler
MESA, AZ POLICE DEPARTMENT

Chief William Fitzpatrick
GLENVIEW, IL POLICE DEPARTMENT

Commander Bruce Folkens
MINNEAPOLIS POLICE DEPARTMENT

Sergeant at Arms Terrance Gainer
U.S. SENATE

Senior Police ID Officer
Stephen Golecki
JERSEY CITY, NJ POLICE DEPARTMENT

Chief Investigator
Adolfo Gonzales
SAN DIEGO COUNTY
DISTRICT ATTORNEY'S OFFICE

CEO Scott Greenwood
GREENWOOD & STREICHER

Police Advisor Robert Greeves
BUREAU OF JUSTICE ASSISTANCE

Lieutenant June Groehler
MADISON, WI POLICE DEPARTMENT

Principal Brett Haan
DELOITTE SERVICES

Major Joe Halman
POLK COUNTY, FL SHERIFF'S OFFICE

Visiting Fellow Kristine Hamann
BUREAU OF JUSTICE ASSISTANCE

Chief Janeé Harteau
MINNEAPOLIS POLICE DEPARTMENT

Assistant Chief Dave Harvey
PHOENIX POLICE DEPARTMENT

Assistant Sheriff James Hellmold
LOS ANGELES COUNTY
SHERIFF'S DEPARTMENT

Vice President Domingo Herraiz
MOTOROLA SOLUTIONS

Assistant Chief Lauretta Hill
ARLINGTON, TX POLICE DEPARTMENT

Deputy Chief David Huchler
ALEXANDRIA, VA POLICE DEPARTMENT

Captain Clarence Hunter
HENRICO COUNTY, VA DIVISION OF POLICE

Assistant Director Harold Hurtt
U.S. IMMIGRATION AND
CUSTOMS ENFORCEMENT

Mr. Roberto Hylton
FEMA

Chief James Johnson
BALTIMORE COUNTY POLICE DEPARTMENT

Lieutenant Matthew Johnson
BALTIMORE POLICE DEPARTMENT

Captain James Jones
HOUSTON POLICE DEPARTMENT

Executive Director Michael Kaiser
NATIONAL CYBER SECURITY ALLIANCE

Acting Sergeant Evel Kiez
CALGARY POLICE SERVICE

Chief Orville King
UNIVERSITY OF CALIFORNIA,
SAN DIEGO POLICE DEPARTMENT

Colonel Steve Kinsey
BROWARD COUNTY, FL SHERIFF'S OFFICE

Corporate Vice President
Kelly Kirwan
MOTOROLA SOLUTIONS

Mr. Rich Kolko
FBI

Captain Laura Lanham
MONTGOMERY COUNTY, MD
POLICE DEPARTMENT

Chief Cathy Lanier
WASHINGTON, DC METROPOLITAN
POLICE DEPARTMENT

Principal Deputy Assistant
Attorney General Mary Lou Leary
OFFICE OF JUSTICE PROGRAMS (USDOJ)

Director Daphne Levenson
GULF STATES REGIONAL CENTER FOR
PUBLIC SAFETY INNOVATIONS

Senior Policy Advisor
David Lewis
U.S. DEPARTMENT OF JUSTICE

Content Developer
Rebecca Looney
NATIONAL LAW ENFORCEMENT OFFICER
MEMORIAL FUND

SAC Ed Lowery
UNITED STATES SECRET SERVICE

Acting Assistant Chief
Lori Luhnow
SAN DIEGO POLICE DEPARTMENT

Director James Lynch
BUREAU OF JUSTICE STATISTICS

Lieutenant Michele MacPhee
NEWARK, NJ POLICE DEPARTMENT

Deputy Director
Kristen Mahoney
BUREAU OF JUSTICE ASSISTANCE

Deputy Director Daniel Mahoney
NORTHERN CALIFORNIA REGIONAL
INTELLIGENCE CENTER

Inspector Daniel Malloy
U.S. CAPTIOL POLICE

Senior Consultant
Thomas Maloney
CRIME ATLAS

Ms. Linda Mansour
OFFICE OF JUSTICE PROGRAMS (USDOJ)

Senior Manager Jason Manstof
DELOITTE SERVICES

Lieutenant Dan Mark
AURORA, CO POLICE DEPARTMENT

Officer Robert Martens
AMTRAK POLICE DEPARTMENT

Captain Shaun Mathers
LOS ANGELES COUNTY
SHERIFF'S DEPARTMENT

Chief Charles McClelland
HOUSTON POLICE DEPARTMENT

Senior Analyst
Debra McCullough
COPS OFFICE (USDOJ)

Assistant Director
James McDermond
ATF

Retired Colonel
Michael McGowan
OFFICE OF U.S. SENATOR
CHRISTOPHER COONS

Chief William McSweeney
LOS ANGELES COUNTY
SHERIFF'S DEPARTMENT

Corporate Vice President
Jim Mears
MOTOROLA SOLUTIONS

Assistant Chief Craig Meidl
SPOKANE POLICE DEPARTMENT

Chief Douglas Middleton
HENRICO COUNTY, VA DIVISION OF POLICE

Chief Kenneth Miller
GREENSBORO, NC POLICE DEPARTMENT

Captain Alfred Miller
PRINCE WILLIAM COUNTY, VA
POLICE DEPARTMENT

Chief Ronald Miller
TOPEKA, KS POLICE DEPARTMENT

Captain Norman Milligan
ANNE ARUNDEL COUNTY, MD
POLICE DEPARTMENT

Program Analyst Pieter Mueller
NATIONAL PREPAREDNESS ASSESSMENT DIVISION

Vice President Tim Murphy
MACANDREWS AND FORBES

Deputy Chief Daniel Murray
ARLINGTON COUNTY, VA POLICE DEPARTMENT

President Rick Neal
GOVERNMENT STRATEGIES ADVISORY GROUP

Lieutenant Kenneth Nelson
SAN DIEGO COUNTY SHERIFF'S DEPARTMENT

Program Manager Martin Novak
NATIONAL INSTITUTE OF JUSTICE

Officer Yaritza Nunez
JERSEY CITY, NJ POLICE DEPARTMENT

Director Denise O'Donnell
BUREAU OF JUSTICE ASSISTANCE

Lieutenant Brian O'Hara
NEWARK POLICE DEPARTMENT

Director William O'Toole
NORTHERN VIRGINIA CRIMINAL JUSTICE TRAINING ACADEMY

Chief Jason Parker
DALTON, GA POLICE DEPARTMENT

Major Mark Person
PRINCE GEORGE'S COUNTY, MD POLICE DEPARTMENT

Officer Samantha Pescatore
JERSEY CITY, NJ POLICE DEPARTMENT

Lieutenant Robert Pistone
HAVERHILL, MA POLICE DEPARTMENT

Public Diplomacy Officer Jody Platt
U.S. STATE DEPARTMENT

Co-Founder Ron Plesco
NATIONAL CYBER-FORENSICS AND TRAINING ALLIANCE

Special Agent Mark Potter
ATF

Captain Maureen Powers
AMTRAK POLICE DEPARTMENT

Senior Administrative Manager Thomas Pulaski
PRINCE WILLIAM COUNTY, VA POLICE DEPARTMENT

Staff Sergeant Asif Rashid
CALGARY POLICE SERVICE

Senior Statistician Brian Reaves
BUREAU OF JUSTICE STATISTICS

Deputy Chief Eddie Reyes
ALEXANDRIA, VA POLICE DEPARTMENT

Captain George Richey
GREENSBORO, NC POLICE DEPARTMENT

Director David Riggs
INDIANAPOLIS DEPARTMENT OF PUBLIC SAFETY

Captain Jim Rizzi
TUCSON, AZ POLICE DEPARTMENT

Senior Program Manager David Roberts
INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Deputy Commissioner Jeronimo Rodriguez
BALTIMORE POLICE DEPARTMENT

Chief Edwin Roessler Jr.
FAIRFAX COUNTY, VA POLICE DEPARTMENT

Captain David Rose
UNIVERSITY OF CALIFORNIA, SAN DIEGO POLICE DEPARTMENT

Deputy Chief William Roseman
ALBUQUERQUE, NM POLICE DEPARTMENT

Detective Chief Superintendent Paul Rumney
GREATER MANCHESTER, UK POLICE DEPARTMENT

Captain Steven Sambar
LOS ANGELES POLICE DEPARTMENT

Officer John Scalcione
JERSEY CITY, NJ POLICE DEPARTMENT

Lieutenant Robert Schroeder
LOUISVILLE METRO POLICE DEPARTMENT

Mr. John Schulze
FBI

Deputy Director Tim Schwering
SPOKANE, WA POLICE DEPARTMENT

Deputy Chief Wayne Scott
GREENSBORO, NC POLICE DEPARTMENT

Detective Brian Shanika
ST. LOUIS COUNTY POLICE DEPARTMENT

Senior Advisor Cornelia Sigworth
BUREAU OF JUSTICE ASSISTANCE

Mr. John Singleton
METROPOLITAN NASHVILLE POLICE DEPARTMENT

Deputy Commissioner John Skinner
BALTIMORE POLICE DEPARTMENT

Deputy Chief Peter Sloly
TORONTO POLICE SERVICE

Manager Steve Smylie
NORTHERN VIRGINIA CRIMINAL JUSTICE TRAINING ACADEMY

Captain Daniel Sollitti
JERSEY CITY, NJ POLICE DEPARTMENT

Major Joseph Spillane
ATLANTA POLICE DEPARTMENT

SSA Herbert Stapleton
FBI

Deputy Chief Henry Stawinski III
PRINCE GEORGE'S COUNTY, MD POLICE DEPARTMENT

Director of Public Safety James Stewart
THE CNA CORPORATION

Retired Chief Thomas Streicher
CINCINNATI POLICE DEPARTMENT

Program Analyst Lauren Sugayan
HAYWARD, CA POLICE DEPARTMENT

Lieutenant Timothy Tew
FAYETTEVILLE, NC POLICE DEPARTMENT

Captain Steven Thompson
PRINCE WILLIAM COUNTY, VA POLICE DEPARTMENT

Chief Alan Townsend
POULSBO, WA POLICE DEPARTMENT

Deputy Chief Hector Velez
PRINCE GEORGE'S COUNTY, MD POLICE DEPARTMENT

CEO/President Maria Vello
NATIONAL CYBER-FORENSICS AND TRAINING ALLIANCE

Chief Scott Vermeer
MOUNTAIN VIEW, CA POLICE DEPARTMENT

Director of Public Safety Laura Waxman
U.S. CONFERENCE OF MAYORS

Major Stephen Waymire
DES MOINES POLICE DEPARTMENT

Director Edward Welch
FEMA – OFFICE OF COUNTERTERRORISM & SECURITY PREPAREDNESS

Chief Paul Williams
SPRINGFIELD, MO POLICE DEPARTMENT

Major Stephen Willis
CHARLOTTE-MECKLENBURG, NC POLICE DEPARTMENT

Chief Michael Yankowski
LANSING, MI POLICE DEPARTMENT

Inspector Carianne Yerkes
MILWAUKEE POLICE DEPARTMENT

CRITICAL ISSUES IN POLICING SERIES

Challenge to Change: The 21st Century Policing Project

Exploring the Challenges of Police Use of Force

Police Management of Mass Demonstrations

A Gathering Storm—Violent Crime in America

Violent Crime in America: 24 Months of Alarming Trends

Patrol-Level Response to a Suicide Bomb Threat: Guidelines for Consideration

Strategies for Resolving Conflict and Minimizing Use of Force

Police Planning for an Influenza Pandemic: Case Studies and Recommendations from the Field

Violent Crime in America: "A Tale of Two Cities"

Police Chiefs and Sheriffs Speak Out On Local Immigration Enforcement

Violent Crime in America: What We Know About Hot Spots Enforcement

Violent Crime and the Economic Crisis: Police Chiefs Face a New Challenge – PART I

Violent Crime and the Economic Crisis: Police Chiefs Face a New Challenge – PART II

Gang Violence: The Police Role in Developing Community-Wide Solutions

Guns and Crime: Breaking New Ground By Focusing on the Local Impact

Is the Economic Downturn Fundamentally Changing How We Police?

Managing Major Events: Best Practices from the Field

Labor-Management Relations in Policing: Looking to the Future and Finding Common Ground

"How Are Innovations in Technology Transforming Policing?"

Improving the Police Response To Sexual Assault

An Integrated Approach to De-Escalation and Minimizing Use of Force

Policing and the Economic Downturn: Striving for Efficiency Is the New Normal

Civil Rights Investigations of Local Police: Lessons Learned

The Police Response to Active Shooter Incidents

POLICE EXECUTIVE RESEARCH FORUM

Police Executive Research Forum
1120 Connecticut Avenue, NW, Suite 930
Washington, DC 20036
202-466-7820
202-466-7826 fax
www.PoliceForum.org

We provide progress in policing.

We are grateful to the Motorola Solutions Foundation for its support of the Critical Issues in Policing Series

MOTOROLA SOLUTIONS FOUNDATION