Webinar Transcript

Addressing Cybercrime

Hosted by the NGA and NCJA
January, 2019
www.ncja.org

Maggie Brunner: Hello, my name is Maggie Brunner. I am the Program Director at the National Governors Association Center for Best Practices over cyber security, emergency communications and technology. Thank you for joining us on the webinar today. Today's topic is what states can do about cyber crime. Just a basic overview of what NGA is. We are a nonpartisan, nonprofit association, dedicated to sharing best practices. We are an association of all the governors. We're divided up into two shops, one is NGA [inaudible 00:00:37] membership and then I sit in the center of best practices, which is a 501(c)(3).

In 2012, we founded the Resource Center for State Cyber Security. This was at the behest of then governor, Rick Snyder, of Michigan. He has been one of the co-chairs of this work. We have had always a one republican co-chair and one democratic, so you'll see here some of the past co-chairs as well. Right now, the current co-chair is Governor John Bel Edwards, of Louisiana.

The Resource Center was founded, again, in 2012. While it focuses on cyber security, it also includes many resources on combating and addressing cyber crime. This is one of our most recent publications that came out this year. It's a top level guide, designed for executives, called, "Cyber Crime: What a Governor Can Do." It outlines current challenges and building capacity for cyber crime enforcement and what the role of the state can be. It includes a lot of recommendations that I'll cover in today's webinar.

What are we talking about today? Today's webinar is going to talk about what is cyber crime and why it's so important. We'll also cover, what are the challenges associated with addressing cyber crime, and what states can do. First topic, what exactly is cyber crime? What are we talking about here? Most folks sort of delineate cyber crime into two buckets. One is high-tech crime, and that's where the actual target is a computer or a network, so that might include crimes such as network intrusion, or like a denial of service attack. Again, these are some of the technically sophisticated ones where we're actually thinking about targeting a computer or a network.

Now, there's also computer enabled crime. This is where folks use the internet or computer to help them fundamentally conduct crimes that have been around for a long time, but maybe conducted in a new way, like fraud or theft. Now this distinction can get a little bit blurry. Let's say, for example, there was a data breach that started off as a network intrusion and then it's used to commit fraud or theft. It's not really a clear line, but what people find in terms of setting this up is that this distinction helps them organize and figure out how they want to prioritize.

Cyber crime is huge and it's exploding. There are limited resources for the government to address it. Some folks really want to take advantage of this landscape. Let's say a state says, "Hey, we're going to focus on computer enabled crimes so that we can free up the feds to really focus on network intrusion and things like that," that may be one way to organize. Then some other folks might say, "You know, we really want to enhance our high tech abilities to really focus on those so that the locals can handle computer enabled crime."

Again, cyber crime is enormous and it's only growing. It's all about prioritization because folks can't tackle everything. Importantly too, nowadays digital evidence is really influencing all crimes. It becomes important too to think about at what point, in terms of organizing a state justice agency, you want to have particular units handle particular things. With visual evidence influencing almost every crime nowadays, you might want to say, "Okay, will major crimes handle this? At what point should we turn this over to a cyber crimes unit?"

Part of the challenge here is that cyber crime is really hard to classify, so regardless of whether an agency uses the UCR or transition [inaudible 00:04:07], it's really hard to capture these computer crimes. Are we talking about is it a theft, where the location was the internet, et cetera? There are a lot of folks, especially like the National Academy of Sciences and some crime modernization task force, looking into this. How do we really classify and count cyber crime? Needless to say, this juncture is really complicated.

I'll just give you an example. Something like swatting. That's a crime where you can use all of these different anonymization techniques from the internet to create basically a false police report saying that there's a really serious situation and a SWAT team needs to be deployed. How would that fall? Would you say that that's filing a false police report and the location was the internet, or the internet helped do it? Again, we're seeing these new crimes emerge and it's not really clear how they should be reported and how we should be counting them.

Also, cyber crime is massively under reported. Federal estimates say that there are only about 10 to 15% of cyber crimes that actually are brought to the attention of the government. Again, we had to think about people incentivizing this behavior. If you have a fraudulent charge on your credit card statement or on your bank account, you might just be able to go to your bank and have the bank say, "Okay, well we'll cover you," so they're absorbing it into the cost of their business. Folks might not be necessarily motivated to bring this to the attention of law enforcement.

Similarly, a business might not want to highlight the fact that they've been breached and so they might not often work with law enforcement. There's a lot of work to be done to really build that trust so that folks, first of all, feel motivated, but second of all, feel comfortable going to a government agency to talk about cyber crimes that they've experienced. It's really important too because it's essential for us to connect the dots. There might be a really small, minor cyber crime, but when you look at the number of victims and you fuse that together, you can see that it's a large scheme and it's really important that we address this and might rise it up in the level of priority.

The internet crime complaint center, I see three. The FBI has done a fantastic job of collecting some of this data and building bigger cases, but more needs to be done. It's also challenging too because a lot of times, in terms of the best way to prosecute or move forward with the case, it might not be classified exactly as the crime that it appears. One example of this is sextortion. That's a crime where folks will breach somebody, get some compromising photos and then use that to harass them in a systematic way, extorting further elicit content, for example.

A lot of times, for law enforcement, it might make sense just to go forward with this case. If the victim is a minor, it's a child exploitation case. A lot of these cases you'll find wrapped up into some of those other types of crimes. It's challenging because that means that you're not really getting a sense, a picture, of how much this is occurring, not really understanding how big of a phenomenon this is.

What we do know is that the cost of cyber crime is increasing. This is actually some data from the Ponemon Institute, an Accenture study. It talks about the cost of cyber crime. As you can see, significantly increasing year after year. In the aggregate, we're seeing a huge jump in terms of the numbers, in terms of the global economy. A recent report from CSIS said it costs the global economy about 600 billion a year.

Aside from financial impacts too, in the aggregate, these are real world victims. There tends to be a misperception in cyber crime that it's just a property crime, so maybe we shouldn't take it as seriously. However, crime victims expect that the police will do something. If they go out of their way to report a crime, they want to see that folks are at least trying to address it. Even if they come across a roadblock, they want to know that there's going to be at least some movement towards this. It can be a really interesting dynamic for law enforcement agencies where they have to manage expectations.

If there is a lot of anonymization happening in this, it might be hard, especially if the perpetrator lives overseas, to really pursue the case to the extent that the victim wants. You have to balance this need to encourage folks to come forward, at the same time with saying, "Okay, well maybe a win for this is just collecting the data." There are also a lot of victims who are experiencing financial crimes and having devastating impacts on their lives. It's not always a case that a bank is just going to refund you. Identity theft can have some severe impacts for victims over the longterm, including on their emotional wellbeing.

It's really important for law enforcement agencies to address this. We can't just let a whole host of perpetrators get away with these crimes without any kind of consequence. I also highlight too, that a lot of cyber crimes are not just financial. We have things like cyber stalking that can have a real, physical impact on the victims, and hurt them from a physical and emotional perspective. What we highlight too is that a lot of government, and particularly justice agencies, are themselves victims as well. From a risk management perspective, it's really important to investigate like a ransomware attack.

We know that those happen at justice agencies pretty frequently, because of the sensitivity of the data that they might have. The other thing too is that from an officer safety perspective, we're talking about crimes like doxing, we see a lot of high profile cases where because law enforcement is out there in the face of the government, they're being attacked in cyber space for that role, specifically. As a justice professional, police executive or a public safety executive, it's really important that you take care of your own people.

In terms of severity of cyber crime too, we're seeing a huge impact as well in critical infrastructure and lifeline services. In 2017, there was an attack that took down the Ukrainian power grid for some time. Ever since then, it's become clear in our minds that the U.S. as well could have a cyber crime that could impact the entire nation. This year, there was a ransomware attack that hit the Colorado Department of Transportation. There was the SamSam ransomware attack that took down about 2,000 computers for weeks. At this juncture, we've heard from Colorado that it's costing millions of dollars and counting to recover from this incident.

Cyber crime is not just something that exists in theory anymore. It's really impacting the United States as whole. We've also seen a lot of instances, and there's a growing concern, about the ability of network intrusion to take down a 911 system. We need to worry about our lifeline services that our citizens depend on.

Now that we've outlined what cyber crime is, what it's not, how people are thinking about it, we're going to talk about some challenges that are associated with it. As I mentioned, part of the problem with cyber crime is that it's technical. Criminals can easily mask their identity on the internet using various forms of technology. We've spoken with some folks who said, "Where we like to focus our resource is on the people who mess up. If you're doing cyber crime well, it can be incredibly difficult for folks to track you down."

Even if you are able to get through these technical hurdles, though, the nature of cyber crime itself is that it can be incredibly global. It doesn't just impact one locality, it can transcend jurisdictions and even nations. As a result of that, if you are able to untangle all the techniques from masking folks' identity, it may lead you to a perpetrator in a different country. There's a complicated process for addressing those types of crimes. It still can be done. Most folks at the state level, though, choose to work through federal agencies so that they can through liaisons and obtain information via the multilateral assistance treaty process.

There are also several federal agencies that can do operations to bring cyber criminals to different areas, et cetera, where they're able to be arrested. For that reason, a lot of state and local cyber crime units really turn to their federal partners via taskforce. Another challenge associated with cyber crime is just competing priorities. We're all trying to do more with less. If you're deciding where you want to invest additional resources, is cyber crime where you want to put it?

Cyber crime units cost money and police resources are strained. Justice agencies are really trying to figure out where is the best use of thinking about their funds. While it might be tempting to say cyber crime enforcement is really a federal responsibility, it's important to note too that no federal agency has the resources to tackle this alone. It's a growing problem. It's effecting citizens and again, the economy in the aggregate. Just like in other cases, regular crime, terrorism, et cetera, we all need to have force multipliers to continue to fight this as a whole.

Within justice agencies too, there are also some specific issues that make it more challenging to stand up a cyber crime unit. What we've heard from some folks on the ground is when they're becoming a cyber investigator, it can take about six months to feel like they're proficient and a full year to really feel like they're comfortable in pursuing cyber cases. An inherent challenge with that is many different police agencies will rotate positions every two years. There needs to be some creativity here and justice agencies need to think about how

they can get this done so that you're not sending someone to the cyber crime unit and thinking that there's going to be somewhere where their career stalls.

Training is also a huge issue as well. Training can be very costly when it comes to a whole different technical things that you need to learn. There's a count that need to keep up to date on the latest techniques. We heard from one police executive that if he trained a cyber unit to the fullest extent that's recommended, it would take their person out of office about one-third of their time. You really need to balance the need for training with a need to also then use that person to conduct investigations.

Importantly, there's also different levels of training that's needed for different parts of the organization. For all officers, it's really important to learn about digital evidence. Digital evidence is impacting almost every case. Officers should be ready to detect it and to figure out how to preserve it. In terms of detection, if you go to a house and you see there's a CD-Rom with about a half an inch of dust on it, maybe that's not something you would need to collect. There's a lot of other potential areas for investigations too that officers should be thinking about.

For example, with the explosion of IOT devices out there, we're starting to see some cases that are being made on the basis of things like Fitbits or other wearables, smart meters, so there's this whole source of data that's essentially being untapped until now. The police agencies are still trying to think about how they can incorporate it into their investigations. It is really essential for all officers, whether they just be first responder, or a detective, to think about all types of digital items that they need to be detecting at the scene.

Also, in terms of preservation, if you collect a cellphone at the scene, for example, and someone remotely wipes it, that's not going to do you much good. There are certain techniques that need to be trained, all officers of an agency, so that they know how to preserve digital evidence as well. This is becoming increasingly important. Because the nature of crime is really changing because in society we're so much more reliant on our smart phone, et cetera, a lot of crimes are being conducted through those means and also those different types of technology that we use are creating a digital footprint.

It's also important for all officers to really think about officer safety. Again, police officers are out there now. They're being doxed. What kind of information are officers putting out online? A lot of justice agencies have released guidance, not only in terms of what you're saying on social media from

the perspective of community trust, but it's also important to think about digital officer safety.

Once you have that first touch training for all officers at the agency, then you really need to think about your cyber unit. Again, this is where it can get really costly and expensive, but if you want a fully trained cyber unit who can conduct investigations, it's essential that they have all the training tools that they need. We'll cover some resources for that a little bit later in this presentation. From there, there's also a need to train folks in digital forensics.

This applies not only to cyber crime, but because digital evidence is also a building block of many cyber investigations, it's important that there's folks at an agency who can really take all of this digital evidence and process it and make it ready for analysis or for court. Right now there's a huge backlog of digital evidence across the country. Figuring out how to make this process efficient and to really put resources behind this is an essential function. Here's where we see, there are a lot of things like a regional computer forensics laboratory, where folks can engage in multi-agency cooperation to help each other out with this.

At the top level, it's also essential for folks to be trained to be able to testify investigative techniques, digital evidence, et cetera, in court. The Daubert standard, we want to make sure that there are folks that can tap into so that they can come and testify. It's not enough to just say, "Okay, I plugged a cellphone in and this is the data that came out." You need to be able to understand the science behind it in order to bring that into court. Here's where we see a lot of states stepping up to help locals too. Maybe local agencies don't have someone certified to testify, and that's where the state can help out. You can also rely on private companies to the extent that they're willing to help you out. We've also seen some folks tap into their fusion center, have trained personal fusion centers who can help the jurisdiction.

What can states do to address cyber crime? One important thing for executives is to think about how you want to message this to the legislature. This might be an area where not a lot of state legislators are very familiar with it. They might not know the cost. They might not know all the impact that it's having on citizens. There is a need to go and advocate for more resources to pay attention to this issue. We've seen in a lot of states that it is police executives who are going and saying, "Okay, here's why I need to have a cyber crime investigator. Here's why I need to have a cyber intel analyst at my fusion center."

That's an important role that executives can play in terms of bringing attention to this issue. Also there's, in some instances, a need to change the laws. There are particular criminal codes that are old and outdated and we really need to think about what can we do to provide maximum deterrents for cyber crime and to really reflect the cost on the people. Again, going back to swatting, as an example. If you call in an emergency, a false emergency, with the intent to harass someone to have a SWAT team deployed out to their house, that's an enormous amount of government resources that's being expended.

It can be rife, a situation where the police don't know what they're going into and they think it's a really dangerous situation and the person in the house thinks that there's a potential intruder, for an officer involved shooting, unfortunately, or a risk to officer safety. If there's no criminal code saying that this is a felony, that's something states should think about and think about holistically because to the extent that this is really impacting society, it might be that there's a need to have additional deterrence.

We've seen in a lot of states that they are starting to codify these things. An example, codify swatting specifically as its own crime so that it can have associated penalties that fit the harm to society. There are also states that are looking at things, like their rules of evidence, to help with admission of digital evidence. Again, it's important to think about this holistically. Not only is cyber crime a special consideration, but digital evidence, that it's building blocks of these cases. There are a lot of challenges associated with that that could be addressed through legal or regulatory means.

We're also seeing that there's a need to really educate the community. Let's not just address these crimes. What can we do in terms of prevention? That's something where law enforcement has been shifting overall. From a government perspective, what touchpoints are you having with the community where you can educate them on things like basic cyber hygiene, safety online? Are folks already going out into schools? Are they already going out into community center? This is a great function for law enforcement as, again, one of the most visible faces of the government.

In terms of their community policing, or relational policing mission, is this something that they could take on to start to train and have this be a conversation? A lot of time in response, you know it is the local officers that are in the best position to offer materials or hand outs to citizens, and again, encouraging folks to report these crimes as it comes up. Does a state or local agency direct people to IC3.gov to report? That's an important thing that we need to think about.

This is a picture of an exercise. As we're becoming increasingly concerned about cyber intrusions that might disrupt government services, or important lifeline or critical infrastructure sectors, there is a need to come up with formal disruption response plans and then to actually exercise them, so that folks know what to do in the event of disruption. Here are some of the training resources that I've highlighted. The United States Secret Service offers an entire academy, called the National Computer Forensic Institute. It's located in Hoover, Alabama. It's free and it has training specifically for officers, prosecutors and judicial officials.

There are also several nonprofits who offer free training too. Of course, the Bureau of Justice Assistance has a great number of resources that can assist justice agencies, if they're thinking about cyber crime. This is just one that [inaudible 00:23:00] cyber center. It's a partnership with BJA, the National White Collar Crime Center, the International Association of Chiefs of Police, Police Executive Research Forum and several other partners. It includes a ton of resources about trainings that are available, sample legal documents, and a whole host of news where justice agencies can learn the latest on cyber crime.

That's the end of my presentation. If there are any questions, please don't hesitate to reach out to us here at the National Governors Association. We are happy to help with any kind of technical assistance request that states may have. Again, to recap what we covered today, we covered what is cyber crime, what are some of the challenges associated with addressing it and what states can do. Thank you for your time. I hope you enjoyed this webinar.