James B. Comey

Director
Federal Bureau of Investigation

Share on Twitter Twitter Share on Facebook Facebook Email Email

International Conference on Cyber Engagement, Georgetown University
Washington, D.C.

April 26, 2016

Privacy, Public Safety, and Security: How We Can Confront the Cyber Threat Together

Remarks as delivered.

Thanks so much, and good morning everybody. Thanks for giving me a chance to share with you some thoughts on behalf of the FBI about all things cyber. Then I'd be happy to take questions after I've shared these thoughts. Let me start by talking about the threat, and how from the FBI's perspective we see and slice the threat: who the actors are, how they're coming at us, and what they're after.

We divide it into five groups. There are lots of different ways to think about this, but the five groups are the nation-states like China, Russia, Iran, and North Korea, and multi-national cyber syndicates—we've seen a significant increase in the size and sophistication of those who are looking to steal information simply to sell it to the highest bidder. The third category that we think of the threat through is the purveyors of ransomware, which is spreading like a virus across the United States and other parts of the world. The fourth group is the hacktivists. That is a motley collection of people who are engaging in computer intrusions for all manner of motivations, some political, some to harass, some financially related.

Then the last bucket is the terrorists. Terrorists have become highly proficient at using the Internet to sell their message and to recruit and plan for attacks. They're quite literally buzzing in the pockets of people to try and make them followers all around the world. There’s no doubt that terrorists aspire to use the Internet to engage in computer intrusions to get to our systems for all kinds of bad reasons, but we don’t see them there yet. Because the logic of terrorism and the Internet is what it is, that’s a threat we constantly worry about.

Those are the five ways we divide up the threat actors that are coming at us through computer intrusions. How do they operate? Increasingly, we are seeing them mount attacks on larger targets, combining multiple techniques, and often exploiting significant inside knowledge of their target. They’re using social engineering to come after all of us, whether that is the government, the private sector, or academia, and they’re using social media to target employees of our institutions in order to try and engineer a way into a system. Every bit of information for these groups of actors is a nugget of gold, every bit of information can be leveraged to gain access.

What are they after? Information, access, advantage, money, all kinds of things. Increasingly, we’re worried not just about the loss of data but the potential manipulation of data, the corruption of data. The threat is not limited obviously to actors on the outside. An important dimension of our cases increasingly are insiders who have knowledge of the system, and not just privileged access. Employees who are willing to sell their knowledge to the highest bidder.

Let me say a few words about the impact of recent attacks. These are more than just attacks on our infrastructure. They’re attacks on the private sector and the public sector, on employees and customers. They’re attacks on reputation, they’re attacks on security, obviously, also attacks on fundamental rights. We see the Sony attack fundamentally as an attack on free speech. This was North Korea unhappy with the content of a particular film that Sony was looking to release, and looked to wipe out that content before it could be broadcast. They quite literally shut Sony down because they didn’t like the content of the movie. That obviously sets a very dangerous precedent.

The behavior of all these threat actors is behavior that we think is susceptible to deterrence. The FBI is working very hard to get us to a place where we are not accepting intrusions as some kind of new normal. We think we have to be more predictive and less reactive, as governments certainly, but also as members of the private sector, and academia. I think there are three main ways to go about being less reactive and more predictive.

First, we can start by reducing our vulnerabilities. For our part, we think the FBI has a role to play in helping people understand what hackers and cyber criminals are after and how they're coming after it. All of us, government and private sector, can harden our targets and better secure our data and our networks. We can make cyber security a priority at all levels.

Second—and this is where the FBI I think has the main role to play—we can work to eliminate the threat. I know we can't eliminate every threat and every vulnerability, but we can find those responsible and hold them accountable, whether through prosecution, publicity, or economic sanctions.

Third, I think we can all focus, if an attack has happened, on mitigating the damage better. I also think there's a role the Bureau can play here, and that is helping people understand what happened in your system. Who did it and why, so you can patch and repair and protect much more quickly.

For the FBI's part, we are focused, as I said, on trying to help eliminate the threat through attribution and imposing costs on the actors. Our strategy to do that is five parts that are pretty simple. The first is we're trying very hard to focus ourselves. There is a challenge in all things cyber, and this is the normal framework through which the FBI views our work: Which physical location? Answering the question, "Where did it happen," and then assigning the work to that field office. That doesn't make a whole lot of sense when it comes to cyber, because often the physical manifestation of the threat is not at the core of the threat. It happens to be seen at a company in Indiana or in Texas.

What we're trying to do is not be bound by that normal paradigm of physical location, and instead ask ourselves, "Who in the FBI is best equipped to respond to this threat? To understand this threat and track this threat?" Then we work to assign that work based on expertise. If the Little Rock office shows great chops in dealing with a particular dimension of one of those five sets of actors, they will get that work. It’s what we call a cyber threat team model. We will assign the threat where the ability is, and then allow four other offices to help based on physical manifestation of the threat, because we still need to interact with the executives of the victim company that work on mitigating the damage to their software.

This cyber threat team model, which we’ve been doing a little over a year now, seems to be working in the FBI. It has created a very healthy competition inside the organization, where people want to become experts in a particular threat so that they own it without regard to where the victims may reside.

The second thing we’re trying to do as part of this internal focus is to bring all of our expertise to bear in our most important matters. We’ve formed something called the CAT, which is the Cyber Action Team, which is made up of experts, special agents, and forensics experts of different kinds from around the organization. They deploy like one of our counterterrorism fly teams, where we will send people to an incident in the United States or anywhere around the world. If there’s a terrorist attack, we’re now doing the same with cyber incidents to focus our resources and our expertise in the same place.

Obviously, and I won’t spend a lot of time talking about this in remarks, we are focusing ourselves to make sure we have great technology for our troops and that we attract and retain great people, which is an enormous challenge for all of us. That’s the first part of our strategy: Let’s focus ourselves.

The second part of our strategy is, how can we shrink the world? The bad guys, whether they’re nation-states or hacktivists or people operating a ransomware syndicate, have made the world very, very small. They’re moving at the speed of light and are able to do work from their basement in their pajamas half way around the world. We’re working very hard to shrink the world within the federal government to be much clearer and more nimble about who does the work. This has involved a great deal of discussion which has been very productive among actors like DHS, the Secret Service, and the FBI, so we have a clear understanding as to who’s doing what. We want to get to a place where it doesn’t matter who a victim calls, just as in terrorism it doesn’t matter where the lead comes in, it’s assigned very quickly to the right people.

Then the most important application of this effort to shrink our world is our National Cyber Investigative Joint Task Force, which sits outside of Washington. The NCIJTF is 20 federal agencies sitting together, sharing information, and dividing up the tasks.

Third part of our strategy is to impose costs. We're shrinking the world, organizing ourselves, and focusing better so that we can make people feel our breath on the back of their neck—physically, ideally, but metaphorically, if they're sitting at a computer keyboard engaging in a cyber intrusion. We try to do this through locking people up, laying hands on people, through naming people and shaming them, and through economic sanctions, so that people understand, whether you're a nation state or an individual, it's not a freebie to kick in a door in the United States and steal what which matters most to us.

Fourth part of our strategy is to help our state and local partners who need every bit as much as we do to become digitally literate, and to investigate all manner of offenses. There are probably people in this audience who have an e-mail from Nigeria asking you to wire me some money. Don't do it, I don't need your money, and I'm not in Nigeria. All manner of frauds are being brought to the attention of our state and local counterparts. We have to do a better job of helping them get the equipment and the expertise they need to react to that. There's some great work going on there between us and Secret Service off of that.

The fifth part of our strategy is the one I was going to spend the most time on, and that is we simply must get better at working with the private sector. You all have heard this, but this is at the core of our being effective, because all the information we need to understand the threat actors, to impose costs on them, and to mitigate sits on private enterprise in the United States. That's a great thing. Ninety-nine percent of the infrastructure is in private hands in this country. If we're going to be effective, they have to tell us things and we have to tell them things in a good way.

According to a recent study, about 20 percent of those in the private sector in the United States who had suffered computer intrusions, actually turned to law enforcement. That means 80 percent of the victims in this country are not talking to us. We have to get to a place where it becomes routine for there to be an exchange—an appropriate, lawful exchange of information between those victims and government. First and foremost because we need that information to figure out who’s behind the attack.

This is where there may be an apparent divergence in interests. A private enterprise may be thinking, “I don’t care that much about who’s behind it, I need to get over it.” If you’re going to avoid being victimized again and again, you need to understand our interests are aligned in finding out who did it and imposing costs. Speed matters here, both for the victim enterprise and for the government, because the threat is moving at the speed of light.

We understand very, very well, concerns about competitive advantage in the marketplace. People who have been victimized worry very much about loss of investor confidence, public perception, and their reputation. We know that they’re worried about what this is going to do to our operations, how we are going to deal with regulators over this as we are talking to the FBI, and is there civil liability? We understand that you are victims, and we will treat private enterprises that have been victims like the victims they are. We have done this many, many times. We know how to minimize the disruption to an operation. We know how to protect privacy. We will not share data about your employees or your operations. We will make clear at the very start, what the rules of the road are, and explain what happens to what you’ve given us, who will see it, what we’ll do with it.

I was the general counsel of two different private enterprises, as you heard, before I came back to government. I know that general counsels are conservative weenies, and that is what they’re paid to do. Ask those hard questions to understand what’s happening, what they will do, what our exposure might be. We will have all those conversations and we understand they’re reasonable conversations. We also understand that it’s not just cyber with you. Often it is cyber plus something else; there’s an HR problem, there is a contract problem, there’s a business supply chain problem, there’s even a radicalization problem.

The beauty of working with the FBI is we are cyber plus as well. We’re cyber plus counterterrorism, cyber plus counterintelligence, cyber plus criminal, cyber plus international. People ask us all the time, “What do you need us to do?” Get to know us before there is a storm. Sony is a great example of tremendous pain for an enterprise, but also an ability on the FBI's part to help them quickly because we knew them. We knew their CISO, we knew IT people, we were there within hours. Every single enterprise in the United States has a relationship with the fire department where they make sure that the fire department understands their facility, understands the general contours of what their campus looks like. My advice to private enterprises, you ought to have that kind of relationship with the FBI. We don't want your content. Even in the midst of an attack we don't want to read your memos, we don't want to read your e-mails. We need to understand how we can quickly get indicators of attack so we can change the actor's behavior.

I want to say a brief word, as I close, about encryption. There's been some minor media coverage of litigation involving the FBI and Apple. In a very, very important way I'm very glad that the litigation between the FBI and Apple in San Bernardino has ended, because it really was about getting access to that phone: a 5C running iOS 9. I know I've said this many times, but I keep saying that is the reason the Department of Justice brought that action to get us access in a very, very important investigation into a terrorist's device. It's good that we have now found a way into that device. It would be bad if the conversation that's been started, ended.

I think it's very, very important that we understand there is a collision going on between values we all share between privacy and security. Privacy is a wonderful thing. I love encryption. I love privacy. I even find it superficially attractive the notion that no one will ever be able to look at my personal device, but here's the conversation we have to have. There has never been a time in the 240 years of our country where privacy was absolute. In our houses, in our cars, in our conversations, we have reasonable expectation of privacy. All those expectations can be overcome with appropriate predication and oversight. We are moving to a place in American life where because we live our lives on these devices as we do, the notion that they will be immune to judicial process takes us to a place we've never lived in before. My only request is that we talk about the cost of that.

A group of companies and executives sent a letter to President Obama last year where they urged him not to do anything to, in their words, "weaken encryption." This is a term that confused me a little bit. They urged him, they talked about all the benefits of encryption. As I read the letter I thought, “Agree, agree, agree, encryption protects us from so many bad people,” but there was nothing in the letter about the cost. I found that depressing, because it meant either these very, very smart people didn’t understand the costs as well as they understood the tremendous benefits, or they weren’t being fair-minded. Either one of those things was depressing to me.

I don’t believe the FBI should tell the American people how to govern themselves. I think the FBI should take the tools we have and use them as best we can, and tell the American people when the tools are being ineffective. That’s what we’re trying to do. I don’t think companies should try to tell the American people how to govern themselves, but we should not drift to a place where wide swaths of American life become off-limits to judicial process without a serious adult conversation.

I’m in this job for another seven years and four months. I intend to continue to try and push this conversation. It doesn’t fit on a Tweet, it isn’t great to have it in litigation, it’s about values. It’s about conflict among things we all care about. It has to be a serious adult conversation. I’ll do my best to facilitate that conversation. I hope you will join that conversation.

As we talk about the cyber threat, I don’t know whether we can get ahead of the cyber threat. I know we need to constantly work to adjust, to be agile and to be humble in the face of a threat that is different than any we’ve seen before. I hope we will continue to have conversation about how we might do that better as we try to shrink the world and impose costs. I hope you will join that other conversation about how do we keep the technology we treasure and get the safety and security that we need. I think together we can figure that out, if we sit down and listen to each other with an open mind.

I think you for listening to me here today, and I look forward to your questions.