James B. Comey

Director
Federal Bureau of Investigation

FBI/Fordham University International Cyber Security Conference
New York City, New York

July 27, 2016

Humility, Adaptability, and Collaboration: The Way Forward in Cyber Security

Remarks as delivered.

It’s great to be back at Fordham and great to see all of you this morning. What I want to do this morning is just share with you briefly some thoughts about how the FBI sees the threat in all things cyber, how we slice up that threat, what we're trying to do about it, and how we need your help, especially those of you who are in the private sector. Then I'd like to take your questions.

Let me start with the overview of the threat and I'll start with, who are the players? At the top of that stack we see increased effort at cyber intrusion by nation-states and near-nation-state actors. China, Russia, Iran, and North Korea are the most prominent players. We also see just in the three years I've been Director a growth in multinational cyber syndicates—criminal groups that are increasingly specialized as to role, and who are stealing information for sale to the highest bidder for criminal purposes.

We see ransomware spreading like a virus. It is simply about a pure business proposition—how much people will pay to continue to do their business. Then hacktivism, which is the term we use for a motley collection of people of all different kinds of motivations, some political, some financial, some just pure harassment. And then of course terrorists, who have highly proficient at using cyber space to proselytize, to recruit, to direct, to inspire, who are quite literally buzzing in the pockets of troubled people all over the country and all over the world trying to move them toward violence,

and who aspire to gain unauthorized access to our systems. They aren’t there yet. They're trying very hard to move in that direction.

How do these threat actors operate increasingly in complex ways? We see the combining of multiple techniques and inside knowledge, especially based on some form of social engineering, using the so-called human vector to get at us, using social media to gather information about employees, and then increasingly taking advantage of insiders. People whom despite their best efforts at patching and defending and segmenting your network have access to the network because they have to have access. They work there. Disgruntled employees, people willing to sell access to the highest bidder or people with axe to grind.

What they're after is obvious: information and access and advantage and money. Increasingly we are worried not just about the theft of data but the corruption of data, and the denial of access to our own data in cases like Sony.

The impact is known to everybody in this room so I won't spend a lot of time on it. These are more than just attacks on our infrastructure. They are more than just attacks on your money. It’s about attacks on employees. It’s about attacks on reputation. It’s about attacks on our economy and security and even attacks on our fundamental freedoms like freedom of speech. The Sony attack was after all an attack on speech. This was not only a nation-state actor; this was a bully trying to stop someone from talking in a way that irritated the bully.

This behavior needs to be called out, it needs to be sanctioned, it needs to whenever possible be prosecuted. What can we do? We know we can't prevent every attack, but we believe this behavior, all manner of cyber intrusion, is susceptible to deterrence because it’s not done high on crack, it’s not done inflamed by a motive to finding a cheating spouse. It’s done with thought and fingers on a keyboard. That offers an opportunity to change behavior, to shape behavior.

To do that we think we have to get a whole lot more—we, the FBI—more predictive and less reactive.

That’s also true with the rest of the government and the private sector. We think there are three pillars to doing this. First we have to see how to work to reduce our vulnerabilities. We in the FBI believe we can contribute there by helping people understand better the vectors of attack, what the thugs and criminals and hacktivists and nation-states are after and how they're coming for it, to enable our private sector partners and our government partners to harden their targets better. We also think by using our bully pulpit we can help all of you convince boards of directors and executives that cyber security has to be invested in at every level. It’s not just about your systems; it’s also about your people.

Second, we think we can help reduce the threat. As I said, we can't eliminate it. We can't eliminate every vulnerability, but we can find those responsible and send strong messages of deterrence to change behavior. Deterrence includes, obviously, means locking people up. It also includes sanctioning people and shaming people to change behavior. Third, obviously the government has an important role to play in mitigating damage after an attack to help people. What just happened to their system so they can patch and repair and get on with life and business.

The FBI, for our part, has a strategy that has five parts. It should be fairly obvious for those of you who know us. The first thing we're trying to do is focus. This means we have to focus ourselves in several different ways. We're trying to focus ourselves with an understanding that the normal model for deciding where to do our work is based on physical manifestations of harm. The bank robbery happened in Chicago, and so the Chicago office will work that. We're trying to focus our work with a recognition that physical manifestation is not all that meaningful a thing when it comes to cyber.

Where did it happen? Is it where the headquarters is? Is it where the first manifestation in a subsidiary was? We've decided that it really doesn't matter where the physical manifestations of a hack are. We think it makes much more sense to assign the work based on power, based on who has the chops to work this particular threat and work it from there. Then allow other offices to help based on a nod towards physical place and physical manifestation.

We're asking ourselves, who are the FBI's best teams equipped to work this threat? Not accidentally, we're also hoping to set up a competition inside the FBI. Our offices will compete to be the dominant player against a particular threat. If Little Rock has the chops, it doesn't matter when the first manifestation of the hack is in a corporate headquarters of New York City. If Pittsburgh has the chops against this threat, it will be worked in Pittsburgh.

The second way we're trying to focus is to recognize that we can't have enough talent in all places. We need to have a focus on teams of experts that we can surge. This was a technique we've used effectively for 25 years against terrorism with fly teams. Experts who are ready to go at a moment's notice to work terrorism cases. We've built cyber action teams made up of all different kinds of experts who can move at a moment's notice to fly to a particular incident.

The third way we're trying to focus ourselves is getting the right people inside the FBI to help us do this work. It will not shock you to know that recruiting is a challenge for all of us when it comes to cyber talent and a lot of you have a whole lot more dough to throw at the problem than I do. We need this great talent in the FBI, not working for you. We need them inside the FBI, and I'm going to give you some of my secrets, but not a lot, because our interests are not aligned here.

We can't compete on money. We have to compete on mission. We can't accomplish the mission if we don't have the talent inside the organization. The challenge we face was summed up by something one of my five kids said to me. One of my daughters said, "Dad, you're the man," and I said, "Thank you." She said, "Dad, I don't mean that in a nice way. The problem is you're 'the man.' No one wants to work for 'the man.'" I think she's right.

Except if people see what "the man" and "the woman" are like in the FBI and the work we get to do, I think I can beat you no matter how much dough you throw at our folks. And we have to start by making sure great talent sees what this mission is all about.

One thing that we're about to do is to hire a senior level data scientist, something we've never done in the FBI. We're going to hire somebody up at the assistant director level to

work with the assistant director of cyber and other senior FBI leaders to do a few things for us. We want this person to help us understand, to provide technical and operational guidance to us to make sure we're doing what we need to do, and to make sure we have the best technology to attract those people to work for “the man,” and just as importantly to help us figure out who are the right people, and how do we fetch them to get them into our organization.

We need somebody who understands every aspect of the world when it comes to cyber—both public and private—to help us find the future and drive decision-making both on a case basis and on a personnel policy basis.

We're also hiring, as you may know lots, more agents and analysts to help us work cyber. Now the challenge for us when it comes to special agents is this: to hire a cyber special agent we need three buckets of attributes. We need integrity. That’s non-negotiable. You can't be smoking weed on the way to the interview. Second, we need physicality. To be an FBI agent, to have a firearm on behalf of the United States, you need to be able to run, fight, and shoot. We need physicality in addition to that integrity. Lastly, to be a cyber special agent we need high intelligence and technical talent.

Those three buckets are fairly rare in nature. We will find people with great integrity, high intelligence, and technical skills that can't do a push-up. We will find people who have high integrity, who can do lots of push-ups, but don't have the technical talent to be a cyber agent. We're struggling with this and we're trying to have enough humility to realize that our world has changed and so the way we think about talent has to change as well. Among the things we're considering is, if we can get integrity and physicality, can we grow and teach our own? Can we have a cyber university inside the government? Or should we think differently about what makes up the cyber squad?

Currently in the FBI, about eight special agents make up a cyber squad. Does it need to be that way? Do we need eight firearms in that cyber squad or can we make teams with a different mix of non-agent talent and agent talent? Now we are going to try all different kinds of things and be open to modification and to failure and to being wrong and then we're going to try again. That is what we're trying to do when I say focus. Better focus

ourselves in a better way and try to focus ourselves on getting the right people inside the organization.

The second thing we're trying to do is shrink the world in two different respects—internally and externally. We have to shrink the world inside the federal government so we are more effective and efficient. And we need to make sure we shrink the external world. You've heard a lot I think over the last two days about the new presidential policy directive. It clarifies the rules of the lanes in the road for those of us inside the government. That will shrink our world so we don't waste time figuring out who needs to do what, we're much more effective and we'll also reduce the confusion with our partners on the outside.

We want to make it irrelevant who you call. You can call the great people of the Secret Service, you can call the great people of the FBI, you can call anybody about a cyber intrusion and we'll figure out who should do what. We'll figure it out now, and provide clear guidance much more quickly than we could before.

As you heard, the DOJ will be the lead threat responder—not the only threat responder, but the lead threat responder working though the FBI and the NCIJTF. Then our responsibility will be to coordinate with others who might have something to bring to bear in responding to the threat. DHS, with their considerable expertise, will take the lead in asset response. They will try to mitigate vulnerabilities and reduce impact. Then the Director of National Intelligence will be responsible for giving all of us intelligence support so we can see where the threat is coming from and what it might mean.

Really this confirms the way that we've been acting, but it makes sure that it’s written down in ink so it doesn't matter who is the leader of group inside the government—the rules come last and our efficiency remains. We also know we have a shared responsibility inside the government and outside. As I said though, that’s not for you to worry about. You need to know only that you need to talk to us. That’s a problem I'm going to get back to in a second.

The second way we're going to shrink the world is by forward-deploying more of our people. This is work that’s been underway since the last time I was here. We're putting

more and more cyber agents and cyber analysts embedded in our overseas offices because although the cyber world seems based only on photons, those human relationships allow us to be faster than we would otherwise. You're going to see a lot more of that from the FBI.

The third aspect of our strategy is to impose costs. We have to lock people up. We send a message that changes behavior as fingers head towards the keyboard. If we can't lock them up we've got to call them up through indictments, through sanctions, through public name and shame campaigns.

Sometimes people say, isn't this shouting into the wind when you indict, say, Chinese actors for criminal theft? After a year-and-a-half my answer is, “No, it’s more than that.” It changes behavior; it sends a wind that changes behavior. There’s a Wanted poster all around the world with a face of a particular Chinese threat actor. That changes behavior. That person might have dreams of going abroad, might have dreams of traveling to visit their children. The fear of the long arm of the law makes a difference.

We've tried to convince people that we have many flaws in the FBI, but we are dogged people. We just gave up on D.B. Cooper. He had to be 90 and he jumped out of an airplane before we were willing to do that. It’s the same reason we brought the indictment against the Iranian actors for the DDoS attacks in '12 and '13—to send a message of deterrence.

Part of this has been a grappling towards a set of norms, especially with the Chinese, to have them understand something. Nation-states gather intelligence. Nation-states always have. We all do it. We'll try to stop you; you'll try to stop us. What nation-states cannot do is steal stuff to make money. That is outside of norms.

We are making significant progress at having that framework be understood around the world. Whether through indictment or prosecution or sanction or publicity, we are working very hard to have people sitting on a keyboard feel us behind them. We need to get to a place where we can get to them as easily as they can get to us.

Our fourth part of our strategy is that we've got to help our state and local partners. There's only so much we in the federal government can get to and our state and local partners are overwhelmed with cyber crime reports of all kinds. People getting an e-mail from me, from my summer home in Nigeria, asking them to wire money to me in Nigeria. All kinds of fraud. The business e-mail scams, they've become a plague. Our state and local partners have to work through us, and if they're going to be effective we must help them though training and technology.

The fifth part is the last part. That's private sector collaboration. This is something we talked about last time I was here, so I'm not going to say a whole lot about this except one aspect in particular.

The majority of our private sector partners do not turn to law enforcement when there is a system breach. That is a big problem. It is fine when they turn to one of the excellent private companies that provide attribution or remediation, but we have to get to a place where it's routine for all of us to work together. For you to call us when there's an intrusion and not just a private sector enterprise.

We understand that your primary concern in the private sector is to get back to business, to get back to where you were. By we, I mean not just the government, but we, all of us, need to figure out who's behind the attack. There may be on the surface a divergence of interest but our long-term interests are tightly aligned. Because if we don't find out who the actors are and impose costs on them, they will be back and they will victimize you and your industry again and again.

What's our strategy for getting you to talk to us more?It's us talking constantly. It's us bugging you constantly to give us a try, to tell you that we've been doing this for years now, and we understand how to do this in a way that doesn't re-victimize someone who's a victim, because that's how we think of you. We do not think of private sector partners who have been victimized by cyber intrusion any differently than we do a victim of a violent crime, a victim of a stalking, a victim of an extortion. We will work like crazy to make sure you are not re-victimized.

We can’t promise you—and we will not lie to you and promise you—that never ever ever will any of your company’s information be exposed publicly if we investigate. What we'll do is have constant conversations with you so you can understand exactly what might happen and what will happen so you can make an informed risk-benefit choice.

This is about building trust over a long period of time. It actually reminds me of the effort we engaged in for a couple of decades to build trust between those with law enforcement responsibilities in the United States and those with intelligence responsibilities. Since the 1980s we've had a statute called the Classified Information Procedures Act, which was enacted to give clear rules of the road, as insurance to the intelligence community that in criminal prosecutions, intelligence equities would be protected.

They never believed it. The people in the intelligence community were very, very skeptical that they could trust prosecutors and investigators with criminal authorities. We had to build that trust, case by case by case.

One of the most important cases in building that trust was the East Africa bombings in August of 1998. In the wake of that bombing, the CIA was doing a lot of work in East Africa trying to figure out what happened, and so was the FBI. What we worked out was that when we went on a search, we would always have an FBI agent there. Nobody from the agency would ever have to testify. There would always be a set of FBI eyes that could testify. We would not burn them. We promised that. We kept that promise in a trial that happened here in the early part of 2001.

That’s a single example but there’s a pile of examples to build that trust. Because the rules matter, but the way people act within that framework matters most of all. What you're going to see from the FBI is a whole lot of conversation where we will say to you, “What are your concerns? Let’s address your concerns.”

We've been at this a long time. We understand your concerns about competitive advantage, we understand that you’re concerned about disrupting your operations, you have concerns about dealing with regulatory agencies, and you have concerns about liability. As a former general counsel, I know that very well. We have been and will

continue to minimize disruptions, to minimize exposures for a victim. We will prove it to you. We're also working very hard to push, push, push information to you.

The last thing I want to say about this is that we also understand it’s not about the breach anymore. This is why I think the FBI has something unique to bring to the table that people don't realize. As the breaches grow more sophisticated and more common, it’s now about not just the breach, it’s about HR concerns that follow the breach. It’s about supply chain concerns; it’s about damage to customers and operations. It’s even about radicalization.

For the company that’s been breached, increasingly, just fixing the breach is like patching a tire with some of that nasty goop you spray into your tire. It'll get you to the gas station but it’s not sustainable for a long-term fix. The FBI brings to bear here as the lead agency for threat response a much fuller tool box that people may realize.

We think of it as cyber-plus. Given the range of our responsibilities, it’s cyber plus terrorism, cyber plus counter intelligence, cyber plus criminal, cyber plus international. The bureau’s footprint is worldwide. We think that brings to the table assets and capabilities that match this understanding that it’s more than just a breach. We'll help you in ways that you may not fully understand. We hope you'll have that conversation to help us explain to you.

What do I need you to do? Talk to us. Talk to us before there’s a breach. All of you who have headquarters buildings with significant subsidiary buildings, the fire department knows those buildings. Because you've done something smart: You’ve made sure that the fire department doesn't need to be figuring out how many floors you have, how many exits you have, where your standpipes are during a fire. They’ve come there, they've seen the layout, you haven't shown them anything secret, but they're able to operate in smoke and save lives in your building. I would urge you to do something similar when it comes to cyber.

The Sony attack was awful. It could have been a lot worse. We had agents and analysts on site there within hours. We knew Sony because they'd taken the time to talk to us beforehand. We knew the people in their IT organization, we knew their CISO. We didn't

know secrets from them. We don't need to know what your business model is, we don't need to know anything confidential, but it’s very, very smart for you who are CISOs to make sure you know who we are, so that like the fire department, we have a general sense of what help you might need in the event of a fire.

I want to close by saying something about encryption because that issue has, for reasons I fully understand, dipped below public consciousness right now, which is fine. That’s a conversation we're going to have as a country, and just in front of a sophisticated audience I want to remind you of why.

In this great country, our founders struck a bargain for us 240 years ago, and it goes like this: Your stuff is private. The Founding Fathers didn’t speak this way; they didn’t use words like “stuff.” I speak this way. Your stuff is private unless the government needs to see it, and with appropriate predication and appropriate oversight, the balance of this country, the balance of liberty is that the government gets to see your stuff, if they really need to, and with appropriate oversight. That’s a bargain tried among other places in the Fourth Amendment. No warrant shall issue except upon showing improbable cause, and no general warrants. That’s our bargain.

We've lived with that for 240 years in ways we may not even fully focus on. No car, no apartment, no closet, no bank was off-limits from judicial authority operating under that framework. Judges even have the ability to force us to say what’s inside our heads, to force us to testify what we saw, what we heard, what we witnessed—again assuming that our other rights are respected.

We're moving to a place where wide swaths of American life are absolutely private. Our devices are moving toward a place of absolute privacy and there’s something seductive about that. Even I, when I heard that, I said, "That sounds cool. No one can look at my stuff. No one can look at my pictures, no one can look at my notes, no one can look at my—I don't keep a diary, but if I did no one can see it.”

Now remember the bargain we have struck. I'm not here to tell you what the answer is to resolve this problem but one thing we have to recognize is that moving to a place where huge swaths of American life are by default out of reach of judicial authority is a

different way to live. We've never lived that way before and it destroys the balance that our founders struck and maybe that’s okay or maybe that’s terrible. That is not for the FBI to say.

The FBI’s job is to tell the American people when the tools you're counting on us to use to protect you aren't working so much anymore. We need to shout from the rooftops but the FBI should not tell people what the answer is, nor should companies that make amazing equipment. They should not be telling the American people how to solve this problem. The American people should be figuring out how they want to be governed. That conversation has to be informed by an understanding of the cost of absolute privacy.

I found very depressing, just depressing—and even more depressing—a letter that a group of technology companies, that technologists sent to the President last year, which laid down all the tremendous benefits of encryption and I agree. There are extraordinary benefits to encryption. I love encryption. What I found depressing about it is, I read the thing multiple times, and not a single recognition of the costs associated with widespread, ubiquitous, strong encryption. That meant to me one of two things. They either failed to see the costs, which is depressing, or they weren't being fair-minded about it, which for smart people in some ways is even more depressing.

I think we have to have a conversation in this county about where we want to be and the FBI’s job is to be a factual input. A lot of people said, "Oh, you're crying wolf. You people have all kinds of great ways to find information." What we're doing, we're using this period of time when the issue is not so prominent in American life to collect the data. We will show anyone who wants to see the impact on our work.

Just to give you one snapshot, our forensic examiners received 4,000 devices in the first six months of this fiscal year, which is October to March. Five hundred of them could not be opened by any means. That’s a fair number given the growth of ubiquitous, strong encryption both for data in motion, data at rest. It’s only going to grow.

In those 500 are criminals who are getting away, victims who will not be rescued. Criminals who are actually getting away by getting themselves reduced sentences

because we are not able to see the full extent of their criminal activity. And we believe that’s a problem.

At some point, encryption is going to figure in a major event in this country. We've got to have the conversation before that happens because after that happens that time for reflection will be significantly reduced and this is a hard conversation. It’s a conflict of two values that we all share. It does not fit in a tweet. You can't shout it at each other. I very much hope that companies and private sector actors of all kinds and ordinary citizens and people of government will look for ways to have a productive conversation about this.

Nobody has the high ground; nobody is a devil. In this conversation we all share the same values. We may weigh them differently but I know that Apple cares deeply about public safety and I know the FBI cares deeply about privacy and security on the Internet. I hope you'll join in that conversation, which means we will probably have to wait until after the election to have this space in American life to have that conversation, and that’s fine. We’ll continue collecting data so we can have that information before a conversation next year.

To close with cyber, as I said we have to approach this with humility, with the recognition that we can't get ahead of all cyber threats, with humility enough to know that the way we think about recruiting, the way we think about technology, is surely going to change and with the humility to know that we at the government must have open minds. I hope together we can make a big difference to protect your world and the entire world. I thank you for caring enough about this to be here today. I look forward to our conversation. Thank you.