The Economic Club of New York

114th Year
628th Meeting

The Honorable Christopher Wray
Director, Federal Bureau of Investigation

October 28, 2021

Webinar

Moderator: Daniel A. Neff
Partner & Co-Chair, Executive Committee
Wachtell, Lipton, Rosen & Katz
Trustee, The Economic Club of New York

Introduction

President Barbara Van Allen

Good afternoon and welcome to the 628th meeting of The Economic Club of New York in our 114th year. I'm Barbara Van Allen, President and CEO of the Club. As many of you know, The Economic Club of New York is the nation's leading nonpartisan forum for discussions on economic, social and political issues, and our mission is as important today as ever as we continue to bring people together as a catalyst for civil conversation and innovation. I want to give a special welcome to members of the ECNY 2021 Class of Fellows – a select group of very diverse, rising, next-gen business thought leaders as well as students from the Columbia Business School and Medgar Evers College.

It's a pleasure for me now to welcome our special guest today, The Honorable Christopher Wray, Director of the FBI. Director Wray became the eighth Director of the FBI in 2017. He began his law enforcement career in 1997, serving in the Department of Justice as an assistant U.S. attorney for the Northern District of Georgia. In that role, Director Wray prosecuted a wide variety of federal criminal cases, including public corruption, gun trafficking, drug offenses, and financial fraud.

In 2001, he was named associate deputy attorney general, and then principal associate deputy attorney general in the Office of the Deputy Attorney General in Washington,

DC. His duties there spanned the full Department of Justice, including responsibility for sensitive investigations conducted by the DOJ's law enforcement agencies. Director Wray was nominated by President George W. Bush in 2003 to be the assistant attorney general for DOJ's Criminal Division, supervising major national and international criminal investigations and prosecutions.

Today's program will begin with opening remarks by Director Wray followed by a conversation, which we are fortunate to have Club Trustee, Dan Neff, as our interviewer. Dan is Partner and Co-Chair of the Executive Committee for Wachtell, Lipton, Rosen & Katz. And we'll end promptly at 1 pm. As a reminder, this conversation is on the record and we do have media on the line. So without further ado, Director Wray, the mike is yours.

Opening Remarks by The Honorable Christopher Wray

Well, thanks, Barbara, for hosting me today. And my thanks to all of you for joining us. I know, if you're like me, we've all just about had it with virtual meetings these days, but I am glad that today's virtual meeting makes it possible for me to talk safely with so many business leaders at a single time.

I say that because partnership with you and your peers has become really an

increasingly key part of how today's FBI operates. That's why, for example, we now have a dedicated headquarters Office of Private Sector, why we have private sector coordinators in every single one of our field offices around the country. And maybe most important why we have teams in operational divisions like our Counterintelligence and Cyber Divisions, thinking constantly about how to protect and work with industry on the specific threats they counter.

And I'm hoping that we'll get into the broader national security landscape during our discussions today, but to kick it off for my opening remarks, I'd like to talk to you about how we're tackling the cyber threat in particular. And not just because October happens to be Cybersecurity Awareness Month, because of course at the FBI every month is Cybersecurity Awareness Month.

Today, I want to talk about how we're seeing the cyber threat evolve and about the new approaches we're taking to address it. I also want to discuss how essential it is for the FBI to work together with you as partners to combat the threat. And then finally, I'd like to highlight some things that you can do to protect your businesses.

So, over the past decade, I would say that the general public probably didn't spend a whole lot of time thinking about cyber threats. Sure, every year maybe one or two major cyber incidents would capture the nation's attention. Of course, they noticed the

Russian government's election interference in 2016. They probably noticed the Chinese government's theft of nearly 150 million Americans' PII from Equifax in 2017. But I would argue it wasn't really until this past year's onslaught of high-profile cyber-attacks that a lot more Americans really started to take notice.

We saw just over that stretch, the SolarWinds supply chain attacks by the Russian Foreign Intelligence Service, the SVR, at the end of 2020. And, of course, the SVR, as many of you know, was back in the news earlier this week. And then the Chinese government's Microsoft Exchange Server intrusions were revealed in March. Then between May and July, we had ransomware attacks against Colonial Pipeline, JBS Foods, and then customers of managed services provider Kaseya.

And while those five were some of the highest-profile attacks, the reality is they were actually just a few among thousands of incidents targeting businesses and other victims in the U.S. and around the globe. So today's cyber threats are more pervasive, hit a wider variety of victims, and carry the potential for greater damage than ever before. And that's why cyber is, and I think has to remain, one of the FBI's highest priorities. And it's going to stay near the top of our list as long as nation-states and cybercriminal syndicates keep innovating.

They're constantly developing new ways to compromise our networks and to get the

most reach and impact out of their operations. And that includes everything from, for example, selling malware as a service, which makes advanced hacking software broadly available to even unsophisticated criminals. It includes things like targeting vendors, which allow them to evade a company's defenses by compromising trusted outsiders with access to the company's network. It means things like accessing scores of victims by hacking just a single managed services provider who has privileged access to all of them.

So we're tracking and countering literally hundreds of national security and criminal cyber threats every single day. Of course lately we're laser-focused on ransomware schemes, particularly those targeting our nation's critical infrastructure. Not only have they wrought havoc on company operations and caused devastating financial losses, but they've also done things like crippled hospital systems, targeted the energy sector, threatened emergency services, shut down local government operations, and I could go on and on.

They're causing real-world harm, threatening national security, our economic vitality, and public health and safety. We're investigating – just to give you a little context on that – we are, at the FBI, investigating over 100 ransomware strains today, and each one of those 100 or so has scores of victims and their impact has been growing. And whether you look at our IC3 stats on company losses from ransomware, or private sector

numbers on the amounts paid in ransoms, I think it's fair to say that the harm from ransomware more or less tripled last year from the year before.

Now, I recognize that, I hope at least I don't have to convince this audience that the threat from criminal ransomware groups has become severe. You know that all too well. But if there's one thing the FBI understands, it's taking down criminal enterprises. And in this context, it's the same, in many ways, as we've done for 113 years. Our strategy centers on prevention and disruption – trying to hit hackers before they attack or before their intrusions can cause major harm.

So, to dismantle them, we're trying to go after them on three fronts. First, of course, we're taking aim at the actors. Working with our foreign partners to identify who is actually responsible for the most damaging ransomware schemes. And when we do that, we take a broad view. So, within ransomware groups, that means everyone from the so-called administrators, which despite the bland and somewhat innocuous name, is a reference to the skilled coders and organizers of ransomware organizations, all the way to the affiliates, which are essentially ransomware-as-a-service users who pay the first group, the administrators, for the right to use the malware.

But it includes other kinds of actors, like operators of services facilitating cybercrime like cryptocurrency tumblers or bulletproof hosting providers, and others. And we're hitting

them with every available lawful tool. So certainly we're relentlessly seeking to extradite them to the U.S. to face justice, but we're also arming our partners in other countries with the evidence they need to arrest and prosecute them abroad.

So first the actors, second, we target their technical infrastructure. So that means seizing or disabling their servers, their domains, botnets, etc. It means disrupting their operations, raising their costs, all while gleaning valuable new intelligence on their activities that we can then share with others, including all of you in the private sector.

A good example of that would be the international operation we led against the Emotet botnet earlier this year, taking down a key facilitator of some of the more pernicious ransomware strains and other attacks. So the actors, the infrastructure, and third and finally, we're going after their money.

Recognizing that virtual currencies are central to ransomware, we trace a lot of transactions back to bad actors. And where we can, we're also seizing the funds, like you saw us do in the Netwalker takedown, or the Colonial Pipeline attack, among some of the more visible, publicly-known attacks. We're also doing things like shutting down elicit currency exchanges. So actors, infrastructure, money, all of them are important individually, but we achieve the biggest impact when we're able to hit and disrupt all three together.

Switching gears slightly, as grave as the ransomware danger is, I find myself having to remind folks that it is, by no means, the only serious cyber problem out there. We don't have the luxury of defending only against the most immediate threat. Our economic prosperity and our national security, of course, depend on innovation, and there is, and I don't think this is an exaggeration, an unrelenting assault on that innovation. We are constantly – constantly – notifying companies of breaches that we've discovered by adversaries looking for valuable information and intellectual property to steal. Stealing from just about every industry you can think of. Finance, semiconductors, biotech, power, I could go on and on.

Unlike ransomware attacks, a lot of these intrusions often go undetected for weeks or months. So we're trying to put a premium on getting those victims quickly. That's a big part of why we put so much effort into building relationships with companies nationwide. What we've seen is that it takes the full range of our resources to battle the threat to innovation.

To just put a little finer point on that, too often when we see a cyber threat and start digging, we find that the same adversary is also working with an unwitting company's insider to target the same sensitive and proprietary information, or they may be going after it through a foreign-controlled company trying to use a corporate transaction like a joint venture or something as a way to get access to the information.

Most of the time, that threat is coming from the Chinese government or companies under the Chinese government's sway. And to say that they're well-resourced would be an understatement. No company is armed to defend against that kind of multi-avenue threat alone. And that's why we've got to be working together.

In fact, in this country – unlike in places like China – most of what we strive to defend lives in the private sector. Not just our innovation, of course, but our critical infrastructure, and all of our personally identifiable information for the most part lives with you. So that's where our adversaries strike. That's where the intelligence we need comes from. And that's why we need the benefit of your insight, your knowledge, your experience. And we've got to work against the threats that are affecting you together, and we are very open to being educated about the way that you see those threats.

But information works best when it's a two-way street. So we're just as eager to share with you what we're seeing. I'm talking about things like indicators of compromise, tactics being used by cybercriminals, and even strategic threat information. And that intelligence takes a variety of forms, from things like bulletins that we share throughout the private sector to the thousands of one-on-one notifications that we find ourselves making to individual businesses.

Ultimately, combining our intelligence with what you're seeing puts you in a better

security posture before an incident occurs. And then when we share indicators with you and then you share what you find back with us, we can do more work with that information and provide the results back to you again. So we, in effect, create a virtuous cycle that makes us all stronger.

So, I've talked a bit about the threat and your role in helping us combat it. As I said, I've also got a couple of suggestions for how you can protect your own companies. First, it's vital to defend in-depth. And what I mean by that is think about it less as just defending your network's perimeter and more as knowing what lies within and what's most important to protect within. The days of hoping that you can have the cyber equivalent of building a high wall to keep intruders reliably out are – I hate to tell you – largely over. To be clear, to be clear, we do need high walls, but we also need to be constantly looking inward to scan for anybody who somehow made it over or under or around somehow those walls. The good news is that companies have never had so many resources at their disposal, like mitigation and cybersecurity firms, to help do that.

The second thing I would offer is that I know a lot of you have already developed partnerships with your local FBI field office, and I would urge you to continue building those relationships with the Bureau and to do so before a crisis strikes. Don't wait. One way you can do that is by partnering with our New York Field Office. You can also join the national institutions we've built up that make sharing more automatic. For example,

we, the FBI, are now co-located with U.S. and international partners in industry, academia, and the financial sector as part of the NCFTA, which is the National Cyber-Forensics and Training Alliance, both here in New York and in Pittsburgh.

When you already know and are really acquainted with your FBI partners before the storm hits, then you go into a storm already understanding how it is we can actually help. How especially when we're able to start investigating right away, we can help stop the bleeding and enable faster remediation with the knowledge that we have about actors' techniques, their malware, and maybe things they've done to other victims in the past.

But the other advantage to getting to know us before a storm hits is it ensures you understand how it is we actually operate and arguably, even more important, how we don't operate. For example, we may not be able to tell you how we learned what we know, but we can usually get you what you need for action, and we will show the same kind of sensitivity and circumspection with the information that you share with us.

We're not going to be descending on you in a bunch of cyber raid jackets. We've even had companies out on the West Coast that have asked us to show up in hoodies to try to blend in a little more seamlessly. And that's just fine. It's not our normal gear, but that works.

Second, I would say we're not looking – contrary to perceptions some places have – we're not looking to just vacuum up mass quantities of your information, and – and I think this is a key point – we're not asking you for information so we can then just turn around and share it with regulators looking into the adequacy of your cybersecurity after a breach with 20/20 hindsight.

Our investigators are laser-focused on the bad guys, and we're looking for technical evidence so we can find those responsible and work with our partners, including all of you, to disrupt their activity. In fact, we're very often coming back to the private sector for help with those same disruptions. The Microsoft Exchange operation that I described earlier is a good example where we were combining our authorities and our relationships with Microsoft and other industry partners to slam shut back doors that the Chinese government hackers had propped open to the networks of literally hundreds of American companies. But we can only hit back against the attacks we know about.

With more than 113 years in the business, the FBI – I think – has earned its reputation as the world's premier investigative agency. But even we can't tackle this threat alone. And we're up against some daunting threats posed by nation-states, cybercriminals, and increasingly sort of toxic combinations of both of those. And we can only prevail with the help of our partners throughout the private sector, namely you.

So thank you for joining me virtually today, and I look forward to continuing this discussion with Barbara and with all of you.

(DISCUSSION - NOT TRANSCRIBED)