3 Takeaways Podcast Transcript
Lynn Thoman
(https://www.3takeaways.com/)

Ep 45: Secret Service Director James Murray: The New Cyber Physical Nexus & How To Protect Ourselves From Cyber Risk

INTRO male voice: Welcome to the 3 Takeaways podcast, which features short memorable conversations with the world's best thinkers, business leaders, writers, politicians, scientists, and other news makers. Each episode ends with the three key takeaways that person has learned over their lives in their careers. And now your host and board member of schools at Harvard, Princeton and Columbia, Lynn Thoman.

Lynn Thoman: Hi, everyone. It's Lynn Thoman. Welcome to another episode. Today, I'm delighted to be here with Secret Service Director, James Murray. I'm excited to find out how the Secret Service trains their agents to be brave, so brave, in fact, that they will literally protect their protectees with their lives. I'm also looking forward to learning how to protect ourselves, our families and our businesses from all the different kinds of cyber risk, including new kinds of cyber risk. One new kind of cyber risk, for example, that I didn't know about is risk to our physical environments; cyber can affect the physical environment through the control systems of cars, elevators and other internet-accessible devices or systems. Director Murray, welcome, and thanks so much for being here today.

James Murray: Well, thanks, Lynn. Thanks for having me.

LT: How did you first become interested in the Secret Service?

JM: As a little boy, I was very interested in joining the military and/or joining law enforcement. My dad was a state trooper in New Jersey. When I was in college, I was in ROTC, so I had a bit of a military commitment afterwards after graduating and then looked at a bunch of different jobs, actually wound up with a smaller federal agency as an investigator. And at the same time, I applied for the Secret Service here, waited a long time back then. Now, we've streamlined our hiring process, but I probably waited about three years until I was hired back in 1995.

LT: Can you tell us about the mission of the Secret Service?

JM: Sure. Our story goes way back to 1865, and legend has it that it goes back to April 14th of 1865, probably a date familiar to your listeners. On that afternoon, President Lincoln's last official act was to authorize the creation of the Secret Service, and obviously, sad irony that just a few hours later, he'd go to Ford's Theatre where he'd be assassinated. Lincoln's decision that day had nothing at all to do with protection of presidents or national leaders, instead, he was trying to address a different kind of threat, and it was a threat against our economy, had to do with counterfeit currency or bogus notes. So, the Secret Service was created to combat that threat, and as such, we were a purely investigative agency for many years, probably more than 40 years, one of the only federal investigative agencies during that time. It wouldn't be until after the McKinley assassination in 1901, when Congress and then President, Teddy Roosevelt mandated that the Service, go ahead and pick up protection of presidents and others as well. Since that time, so about 120 years now, we've had this dual or integrated admission of both investigation and protection, and

we find that one serves to enhance the other. I hope to be able to talk about that a little bit here with you today.

LT: Can you tell us more about the protective mission?

JM: It's greatly expanded from what it was in 1901. Actually, just to give a snapshot, if you go back 50 years, to about April 1971, for instance, Secret Service probably had maybe around 1,500 agents and maybe about 500 uniform division or what we used to call White House police officers. We probably had a total of 12 protectees or persons that we protect permanently. I should explain that. Our mandate is we protect not only the President and the Vice President and their families, but also other national leaders here as directed by the President, and then we're all so charged with protecting foreign heads of state and heads of government when they travel here to this country. And we also serve as the operational lead agency for these things called National Special Security events, things like the UN General Assembly or the inauguration.

JM: Anyway, back in '71, those were our total numbers. Today, here in 2020s, we have more than 40 permanent protectees, and that's a number that continues to increase. We have probably twice as many agents, it'd be about 3,400 or so, and we probably have maybe 1,500 more officers. And then the balance of our agency, totaling 7,700, are mission support personnel. If you look back, there's a lot of growth within the agency, but it doesn't really match the expanded mission requirement with conducting protective operations in the 21st century, obviously, just in terms of footprint and planning and in layering, it's night and day from what we did many years ago.

LT: It is almost exactly 40 years since John Hinckley attempted to assassinate President Reagan.

JM: Yes.

LT: President Reagan had just given a talk at a Washington DC Hotel and he was leaving when Hinkley opened fire. Secret Service agent Tim McCarthy was shot as he shielded President Reagan with his body. How do you train people to be so brave?

JM: It's funny, I don't know if we train them to be brave. To be candid with you, we really do seek to hire highly capable and highly competent individuals, but we are not kidding ourselves, we don't hire superheroes. We don't expect people to rise to the occasion, we expect them to fall back on their training. Our training is pretty extensive, and candidly, if we have one complaint at all is that we don't have more time to train because of the tempo of our protective mission and the number of people that we have. But I think an answer to your question, there's a certain vocational spirit to do in this kind of work, we are a law enforcement agency, but we're different from others. We operate a lot like the military, but we're not part of the armed services. We are a federal agency, so therefore, we are bureaucracy, but we're different from other federal bureaucracies, in that we don't have any political appointees in the Secret Service. That's by design, because we don't subscribe to any political party, ideology, platform, instead, we are committed to the Constitution. For one to take on a job like this, that's where they have to be coming from. It can't be a partisan effort; it has to be something where you want to be part of something bigger than yourself.

LT: Can you tell us more about the investigative mission? What does it include?

JM: We're still involved in that fight against counterfeit, as I mentioned, still a challenge, especially

when it comes to international stuff. But back in the '70s and '80s, we began to get involved in the fraud game. What I mean by that is as the world's financial system started to digitize, we got involved with things like credit card fraud and what we used to call computer fraud and bank fraud. And, over time, we've developed a particular specialty and focus on that. Back in the mid-'90s, we started something called the Electronic Crimes Task Force in the New York field office, that was the year I started in that office. We've grown quite a bit in that effort, where we have more than 40 task forces, which we refer to as Cyber Fraud Task Forces, nowadays, 40 plus here in the US and a couple overseas as well. So, we're very much involved in the fight against cyber crime.

LT: Can you talk about the different kinds of cyber crime, financial crimes, ransomware infrastructure?

JM: A big one, you already mentioned is ransomware. I think a lot of your listeners will be familiar with what that is, that's quite literally bad actors, cyber criminals gaining access, infiltrating system of systems in order to gain leverage or gain control of certain permissions and thereby taking information or access hostage. They take it hostage for the purpose of either exposing information or extorting people for payment. That is something that's been on the rise over the last decade or so and continues to proliferate, if you will. Along with that is something we're dealing with a lot nowadays, called Business Email Compromise. Business Email Compromise is a combination of a number of different fraud schemes where if you think about the spam email you might get in your inbox. Somebody actually does some research on the company, identifies some patterns within their business systems, they send targeted emails to people within that corporation posing as other people, and they gain more information, they gain more trust. And before you know it, they effectuate something like a payment misdirection, so to speak, or they change wire transfers to go to different locations. That's something we're seeing quite a bit. Along with that, we still see the phishing schemes that we've seen for so many years. We still see credit card fraud in the sense that there's a lot of card skimming going on out there as well.

LT: How has the investigative mission changed over time?

JM: I would tell you that in my career, it's changed and that when I came on the job, it was primarily focused on counterfeit and on, I won't say simple fraud, but credit card fraud, plastic and paper. Nowadays, the lion's share of what we do takes place in the digital world. We are digital investigators first and foremost, notwithstanding the fact that we still do have this mandate to investigate things like counterfeit. What's interesting about how we approach our investigative mission is that unlike other agencies who may decide to work on a specific violation, let's just say bank fraud, or they may work on a specific group, maybe it's nation state actors from a particular part of the world. We don't really approach our investigative mission that way, we look at it from a standpoint of, we are endeavoring to safeguard our nation's financial infrastructure. So you might wind up getting to the same place, but that's where we're starting out from. And in that way, you might be able to see there's a bit of a corollary in how we carry out our investigative and our protective mission. It's really about prevention, awareness, mitigation of risk and so on, on both the protective and the investigative side of the house.

LT: How do you provide 360 degree coverage?

JM: If we're coming to any town, USA or any town in the world, what we're going to do is we're going to send out an advanced team as soon as we know about the visit. We're going to go out, not

by ourselves, let's use a President, we can use any president. You travel to that city and you travel in kind of locked arms, so to speak, with the advanced team from the Presidential staff, also partners from the White House military office, and you'll arrive well ahead of time, you're talking weeks, if not more, depending on the nature of the visit, and you'll start developing a plan with regard to how to safeguard and make secure that visit and that visit may include a number of different site locations or it might include one or two.

JM: In any case, what you do is you assign different people to advance each of those sites, and then you build a security plan around it. And the most critical part of that security plan is, as you pointed out, having 360 degree coverage. You do that through the use of physical measures, things like fencing and barriers, road closures, signage, and then the appropriate use of law enforcement officers and agents to pick up post, so to speak. But in achieving 360 degree security, there's also, in the 21st century, a virtual element of that, and it's ensuring that you are not going to be compromised with all the various systems that exist within a particular venue or a building. For instance, if we're going to an office building, we have to be aware that nobody can hijack the elevator system, the HVAC system, the fire, life and safety systems in place, the electricity and so on and so forth. And we actually have a specialized unit, we have a lot of investment in fighting cyber crimes, we've also invested a lot in what we call our Critical Systems Protection work. We have cyber folks who work specifically to address those challenges.

LT: Can you talk a little more about the cyber physical nexus and how you think about that and protect?

JM: What we want to do is make sure that there's no ability to remotely exploit things like lights, cameras, security systems, elevators, and you want to make sure that all of those efforts dove-tail into those physical measures that you're putting in place. On top of that, if you want to overlay that there's a whole threat management piece that the Secret Service carries out that I think some of our listeners may know about when it comes to people who make threats or may pose a threat to the people or the places that we protect. So all of that goes into the crock pot, so to speak, to build up our protective advance.

LT: So it seems like there are so many different opportunities for cyber criminals and cyber hackers. SolarWinds was an ingenious hack.

JM: Yes.

LT: Where cyber criminals, as you know, hacked the company SolarWinds and installed malicious software that was then downloaded to 18,000 SolarWinds' clients, including the State Department, the Treasury, and blue chip companies like Microsoft, when they updated their SolarWinds software. How do we protect against cyber and attacks like SolarWinds or ransomware attacks?

JM: When it comes to something like SolarWinds, it's a very serious matter, and it's not only a national, but an international concern. It's going to require not only a whole of government approach, but also us working very closely with our Five Eyes partners. And I think it's also going to require a lot of foreign policy investment because just to be clear, what you're talking about in the case of something like SolarWinds is something where these cyber actors, these transnational organized criminal groups, working either at the behest of or in concert with nation-state actors, to carry out what you just described. Those nation-state actors are not looking to build harmony,

they're looking to create a multipolar world order. They look to create discord. So the first thing that any organization can do is build within that organization a culture that is risk-aware, and every organization, if they haven't done so, needs to identify somebody with whack, so to speak, who can champion the cause of cybersecurity across all lines of business.

JM: Another thing that organizations need to be aware of, both public and private, is none of us as individuals or as companies, none of us can go it alone. We're highly reliant on other services and other vendors. So whether we realize it or not, we inherit the cyber risk of other vendors. That same person who's ensuring resilience and continuity of operations within an organization needs to be ensuring that the vendors that any organization is using is doing the same, and that vendor is not willing to share that information or talk about the measures they do have in place, I would suggest finding a different vendor.

LT: How can individuals protect themselves from cyber and cyber physical threats?

JM: We throw around this term called cyber hygiene, and it's just doing the basics. 26 years in the Secret Service, I certainly have more of a working knowledge when it comes to cyber crimes, but I am not a cyber expert, but when it comes to protecting ourselves, it's doing the basics. It's using strong passwords. Seems silly, I realize, using things like multi-factor authentication, making sure if you're using a certain company's cellular phone and there's an update that comes in that you update it. That's the best thing we can do, and it's the simplest thing we can do. And that's the best we could do to stay one step ahead because you have to remember, as sharp and as smart as these cyber criminals are, they are looking for the easiest fish to catch. They are not out there looking for the biggest fish. They're looking to find the easy prey. So when you do those things and you stay on top of cyber hygiene, it's going to work to your advantage.

LT: How do you think about or measure success in cyber?

JM: That's a great question. It's tough to view it in terms of success because from a law enforcement standpoint, obviously, we can lay down yardsticks and measure out our productivity and what we've accomplished, but you have to view fighting cyber crime in more of a holistic stance. It really does require not just law enforcement, not just the government, but all stakeholders, public and private kind of working together. I think we have to educate the public and all sectors of the economy that you need... We are most eager to help those who want to help themselves, because those are the ones that can most easily protect themselves moving forward.

LT: Can you talk about partnerships? How you work with other parts of government, law enforcement and private companies?

JM: As I mentioned earlier, the Secret Service is by design a pretty small agency. We're about 7,700 strong, although we're growing. We're on a path here over the next five years to get up to around 10,000. So if any of your listeners are interested, please check us out on usajobs.com we'll be hiring [chuckle] for a few years to come. But we are highly reliant on our federal, state and local partners when it comes to everything we do, both on the protective side of the house and on the investigative side of the house. We always have been, we always will be. And the reason for that is when we do want to bring the President or the Pope or anybody else to your town USA, it doesn't make sense for us to come in with all of our agents and displace all the strong public safety and law enforcement folks that we have in town, rather we want to leverage what they have and what they

know, and that's what we do. So when we come to town, quite frankly, the wheels don't roll, unless we have a strong partnership and support from the city, state, local police, public safety folks, fire department and so on.

LT: You talked about good cyber hygiene. Are there any documents or links that you could share that listeners could look to to improve their own safety and lower their cyber risk?

JM: I could send them to our public facing website, secretservice.gov, and on there is a whole host of information about best measures to protect yourself and protect your companies big and small and further points of contact.

LT: That sounds terrific. Is there anything else that you would like to mention that you haven't already touched upon before I ask for your three key takeaways?

JM: I don't think so, I appreciate the opportunity to talk about the Secret Service and the high caliber workforce that we have here. I could tell you, I've been doing this for 26 years, and I joined the Secret Service because of the mission. I've thought many, many times to leave, and I stayed because of the people. It's a group of people who are committed not only to the mission, but very much to each other, and that's what makes it a fantastic experience. Candidly, Lynn, it's the best job in the world, because I want to be here. If I didn't want to be here, I think one can make an argument it might be the worst job in world, but because I want to be here, it's the best job.

LT: What are the three key takeaways that you'd like to leave the audience with today?

JM: First is very simply, the fight against cyber crime and achieving anything like cybersecurity requires a whole society approach. It does require a strong partnership between public and private organizations. And the one thing that I want the listeners to understand is they should not just expect law enforcement or the federal, state or local government to just on board and fix this problem on its own, it requires everybody's assistance. Second thing is an observation I've made over the past quarter decade working here, and candidly, embarrassed to say I wish I realized it a lot earlier, and it's quite simply that attitude is everything. It's not only the story of each of us, but it is one that we write ourselves, and it is the key ingredient when it comes to building one's own character that other folks are most attuned to. And it's the one they're evaluating when they decide whether or not they want to invest in us or if they were really going to buy what we're selling.

JM: The last take away is very much more of a personal one. About two years ago, I lost my little brother Ryan to cancer, about four weeks ago, I lost my dad to COVID. Two really special people, really cool individuals, each in their own way, had this unique ability to wherever they found themselves, make that their favorite place to be. So that's what I'm striving to do. That's my new commitment, my recommendation to your listeners is wherever you find yourself, make that your favorite place to be.

LT: I'm so sorry.

JM: Oh, thank you. Thanks very much.

LT: Thank you so much, Director Murray, for our conversation today and for all you and the Secret Service do to protect us, our leaders and the foreign leaders who visit the United States. Thank you

for keeping us all safe.

JM: Thank you, Lynn. Thanks very much.

[music]

OUTRO male voice: If you enjoyed today's episode and would like to receive the show notes or get new fresh weekly episodes, be sure to sign up for our newsletter at 3takeaways.com, or follow us on Instagram, Twitter and Facebook. Note that 3takeaways.com is with the number three, three is not spelled out. See you soon at 3takeaways.com.