CITY COUNCIL
CITY OF NEW YORK

---------- X

TRANSCRIPT OF THE MINUTES

of the

COMMITTEE ON SMALL BUSINESS
JOINTLY WITH TECHNOLOGY

---------- X

February 25, 2020
Start: 10:18 a.m.
Recess: 1:03 p.m.

HELD AT: 250 Broadway, Committee Room, 14th Floor

B E F O R E: Robert F. Holden
Chairperson
Committee on Technology

Mark Gjonaj
Chairperson
Committee on Small Business

COUNCIL MEMBERS: Committee on Technology
Robert F. Holden
Costa Constantinides
Peter A. Koo
Brad S. Lander
Eric A. Ulrich
Paul Vallone
Kalman Yeger

Committee on Small Business
Mark Gjonaj
Stephen T. Levin
Bill Perkins

Ydanis Rodriguez
Helen K. Rosenthal

A P P E A R A N C E S (CONTINUED)

John Paul Farmer
Chief Technology Officer
Mayor's Office

Quiessence Phillips
Cyber Command

Donald Giampietro
Assistant Commissioner
Small Business Services

Daniel Golansy
CEO
Atacama

Steven Bellavin
Professor of Computer Science at Columbia University

Derek Shanahan
Paladin Cyber

STEVEN SIDOWSKI: This is a microphone check. Today's date is February 25, 2020, on the Committee on Small Business jointly with Technology, recorded by Steven Sidowski

CHAIRPERSON HOLDEN: Good morning. I am Council Member Robert Holden, chair of the Committee on Technology. I am pleased to be joined by the Committee on Small Business, chaired by my good friend, Council Member Mark Gjonaj. Thank you for being here and at this hearing. Today we'll be focusing on cyber security for small businesses in New York City and we'll look to gain a better understanding of the cyber security landscape, as well as the cyber security challenges our small businesses face in an increasingly connected world. Cyber attacks are becoming more common and more sophisticated as online technologies continue to evolve, including, but not limited to, cloud computing, artificial intelligence, and 5G wireless connection. More and more our personal data is being found online and businesses are increasingly establishing an online presence as well. Despite being essential for moderate society, having an online presence does have its consequences. In a

2019 report cyber security experts predicted that cyber crime would cost the world 6 trillion annually by 2021. In 2012 then-director of the FBI, Robert Mueller, stated that there are only two types of companies, those that have been hacked and those that will be. Further, he stated that in the not-to-distant future the cyber threat will pose the number one threat to our country. Since those remarks, cyber attacks have become one of the top threats in our country. In 2017 Equifax suffered a breach, exposing crucial information of millions of people. In 2018 the City of Atlanta experienced a cyber attack that disrupted many of its city services, including the nation's busiest air port. And in 2019 cyber attacks crippled Baltimore's 911 call centers. There are also thousands of other attacks, ranging from small scams to huge data breaches affecting everyone from a single person to multinational corporations. And there are no signs that these attacks will be slowing down in any time in the near future, especially as our society becomes increasingly dependent on online technologies. As such, it is extremely important to prepare and be prepared for these threats of cyber attacks. We look

forward to better understanding of how the city can better serve its residents and small businesses on the issue of cyber security, as well as understanding the current state of small businesses in the City of New York. We wish to work together with the administration on this important issue and look forward to hearing valuable testimonies from the administration, experts, and community advocates. I'd like to recognize members of the Technology Committee. We have Council Member Brad Lander, sitting to my right, and, ah, I'd like to turn it over, oh, I also want to thank the staff of the Committee on Technology, counsel Irene Bahovsky, policy analyst Charles Kim, finance analyst Florentine Gabor, and my companies, Daniel Kazem, standing by the door. I will now turn it over to my good friend and co-chair, Council Member Gjonaj.

CHAIRPERSON GJONAJ: Thank you, Chair Holden. Um, good morning. I'm Council Member Mark Gjonaj, chair of the Committee on Small Business and I'd like to welcome you to our joint hearing with the Committee on Technology, chaired by my dear friend, Council Member Holden. Our hearing today focuses on cyber security for small businesses and how we can

ensure our small businesses, in particular micro businesses, the mom and pop shops, are educated and protected from cyber attacks. Small businesses are integral to our economy and culture in New York City. According to SBS, approximately 90% of the 220,000 businesses in New York City employ fewer than 20 employees, generating millions of jobs and bringing in billions of dollars in revenue, reviving neighborhoods and revitalizing regional economies. Micro businesses, which are businesses that employ less than 10 employees, capture more common conception of the mom and pop shop, invoking images of locally-owned retail operations, like barbershops, pizzerias, or local bodegas. Despite mom and pop shops being a vital aspect of our city's unique and vibrant culture, small businesses are finding it more difficult to keep their doors open and stay in business. From the rise of e-commerce the big box store competition and consumer behavior changes, our small businesses are facing more and more hurdles. Cyber security attacks are a relatively new but devastating challenge small businesses must confront. Developing a cyber security infrastructure has therefore become another new difficulty for mom and

pop shops, forcing them to devote time, energy, resources in order to ensure that they stay in business. While cyber attacks are traditionally seen as affecting Fortune 500 companies, every private business regardless of size is at risk. According to the Parliament Institute, small and medium size businesses have reported a significant increase in targeted cyber security breeches for the third consecutive year. Over 40% of online attacks are now aimed at small business. Yet only 14% of those businesses are prepared to defend themselves. A research firm focusing on small and medium size businesses found that 60% of small businesses fold within six months of a cyber attack, 60% fold after a cyber attack. I understand New York State has taken steps to protect our small businesses from cyber attacks. The state's small business development centers produced a guide for small businesses including resources on how mom and pop shops can protect themselves from cyber attacks. Additionally, the passage of the Shield Act shows that the state is aware and working to protect businesses from cyber, and cyber security. I look forward to learning about the steps Cyber Command and the SBS have taken to

educate and protect businesses at the city level. Our government is often reactive, but I look forward to working with our partners to take a proactive stances on protecting small business from cyber attack. The danger posed to small businesses by cyber attack is very real. And it is, has arrived. With this oversight hearing being itself indicative of its imminence, we must meet the challenges head on in order to protect consumers, our residents, our visitors, and the backbone of our economy, our small business. The information from this oversight hearing is the first step towards combatting this threat. With that said, I want to my chief of staff, Reggie Johnson, our legislative counsel, Stephanie Jones, policy analyst Noah Mixler, and our Committee on Technology staff Irene Bahovsky, and Charles Kim for all their hard work in preparing for this hearing, including my co-chair, whom I'm very fond of, Councilman Holden. So thank you so much.

CHAIRPERSON HOLDEN: Thank you. We have a love fest here. Thank you. Um, we've been joined by Council Member Constantinides, and I want to thank the chair, Mark Gjonaj, for those kind words. And I'd like to have the first panel receive the

affirmation. We have John Paul Farmer, he's the chief technology officer of the Mayor's Office, Donald Giampetro, SBS, Small Business Services, and Quiessence Phillips from the New York City Cyber Command.

COMMITTEE COUNSEL: I would like you to raise your right hand. Do you swear or affirm to tell the truth and answer, answer honestly to council member questions? Thank you. You can start.

CHIEF TECHNOLOGY OFFICER FARMER: Good morning, council members, Chair Holden and Chair Gjonaj. I appreciate the opportunity to be here today with my colleges, Quiessence Phillips of Cyber Command and Donald Giampetro of Small Business Services, to testify on the city's initiatives related to cyber security for New York City's small businesses. My name is John Paul Farmer and I serve as the chief technology officer, or CTO, of the City of New York. The Mayor's Office of the CTO works to ensure that advances in technology support government's efforts to solve the most pressing issues in New Yorkers' lives, today and in the future. Foundational to the city's approach is the concept of digital rights, which has been developed

since 2018 through the city's Coalition for Digital Rights, an international network developed by New York alongside Barcelona, Amsterdam, UN Human Rights, UN Habitat, and others. The Mayor's Office of the CTO developed our digital rights principles, cyber security, privacy, equity, choice, affordability, quality, accountability, ethics, and nondiscrimination, and words guide the city's policy, research, programming, and engagement on core and emerging technologies. These principles are critical to supporting not only individuals, but also entrepreneurs and small businesses. These principles are critical to support not only individuals but also entrepreneurs in small businesses as they navigate our increasingly digital society. New York City is positioning itself to be a global leader in cyber security jobs, skills and information, innovation, excuse me. City agencies are creating complementary cutting-edge resources to serve small businesses specifically. We recognize that small businesses face a unique set of challenges and are vulnerable to threats, some of which include email phishing, malware threats, and cyber incidents. In 2018 the Mayor's Office of the CTO along with partner

agencies, the Economic Development Corporation, Cyber Command, and Small Business Services, launched what we call a moonshot challenge on this very topic - cyber security for small businesses. During the development of this moonshot challenge the city engaged technologists from all across the globe and focused the private sector on creating tools to support the city's small business community and increase cyber protections for businesses and customers alike. First, I'd like to describe the Moonshot Challenge program, which is inspired by the words of President John F. Kennedy and the decade of progress that enabled humanity to put a person on the moon. In what became known as his moon speech JFK said we choose to go to the moon. We choose to go to the moon in this decade and do the other things, not because they are easy but because they are hard, because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone and one which we intend to win, and the others, too. That's the mindset of the Moonshot Challenge, to embrace the challenge of doing hard things. And to do it together. Beginning

in 2017 the Mayor's Office of the CTO and EDC partnered to offer these moonshot challenges as an opportunity for innovative entrepreneurs, often small or startup businesses themselves, to work with the city and addressing real-life civic challenges by delivering groundbreaking tools and applicable business models to transfer and improve the way we live. Due to the scale of New York City and the rapid pace of technology development in the private sector there has for too long existed a gap between the city's ability to access innovative products generated by startup entrepreneurs and the interest and ability of these entrepreneurs to create products that are meaningful and impactful for the city. Moonshot challenges create an avenue for just such companies to advance new tools and technology products that solve New York-specific problems. Each winner of these challenges receives an award and sometimes the chance to pilot their product with the city. Past moonshot challenges have resulted in internet connectivity for Governors Island and electric vehicle charging stations tailored to our city streets. New York is leading the way in how cities engage entrepreneurs in urban problem-solving.

We see the moonshot challenges as an opportunity to attract expertise in innovative thinking from small businesses into government agencies. As New York City's roughly 230,000 small businesses transition customer engagement to online platforms we know that it is critical that these businesses are resilient to cyber attacks in order to protect both owners' livelihoods and the personal information collected from customers. In developing our moonshot challenge the CTO's office, EDC, and our partners conducted more than 30 workshops as well as interviews with 50 experts from think tanks, academia, industry, and city government here in New York City and abroad. We also surveyed New York City's small- to medium-size businesses, otherwise known as SMBs. From this research that we did it became clear that there is a significant opportunity to improve the cyber security of SMBs. We learned that these SMBs, one, believe that cyber security is important to their business, two, are dramatically underresourced and underprepared for future threats. And, three, are enthusiastic about adopting cyber solutions. We also learned that there is a gap in the market for tools that are affordable to and appropriate for use by

small businesses. Many cyber security tools, as has been noted, are priced and scaled for larger companies that have extensive in-house security expertise and substantial financial resources. We felt a need to address these concerns by small businesses and so our focus for this moonshot challenge became clear. How might we make every SMB in New York City as resilient to cyber security threats as a Fortune 500 company? Drawing on the expertise of Cyber Command and Small Business Services, we launched the cyber security moonshot challenge to incentivize cyber companies and startups to develop, test, and build cyber security solutions targeted for New York's small business owners. Specifically, we looked for tools that are affordable, effective, and easy to use. We wanted these tools to reflect industry best practices around threat prevention. To ensure that New York City benefitted from innovative thinkers across the world the city partnered with Jerusalem Venture Partners, JVP as it's known, and organizations from Israel, Japan, South Korea, Singapore, Berlin, Helsinki, London, and Paris in order solicit and evaluate proposals from companies and startups. The city also

engaged the Global Cyber Alliance, an organization founded by the New York County District Attorney's Office, the City of London Police, and the Center for Internet Security as partners to promote awareness of the challenge among startups internationally and across the United States. The cyber security moonshot challenge generated over four times the number of applicants relatively to previous challenges, four times. And that was due to these partnerships that were formed. Overall, we received 169 proposals, from applicants in 77 cities, representing 18 different countries. Challenge finalists deployed software prototypes that underwent second assessments by select SMBs and city agencies. Applicants that made it to final round were invited to New York City to engage with partners and to pitch their tools to the Challenge Evaluation Committee. We were happy to have Chair Holden's staff in attendance at the culminating event for finalists. The challenge finalists were a diverse group, familiar with the needs of small businesses and urban issues alike. A few statistics. Thirty-six percent reported being operated by a woman or minority owner. A majority of applicants were early-stage businesses

with 75% earning less than one million dollars in annual revenue. And 93% of applicants reported previously having worked with small- to medium-size businesses. After rigorous evaluation and testing, we selected three winners that provide solutions that are affordable, holistic in their security offerings, easily deployed without a dedicated IT professional, and high-quality in user experience, in language offerings, and in accessibility. As part of the challenge, as planned, the three winning companies received financial awards. Through our research, application process, and selection of winners the city increased its knowledge of small business needs and market offerings. We are using these learnings to inform the city's continued support of businesses. In addition to the challenge, the administration is deploying a host of resources to ensure that New Yorkers are well equipped to deal with cyber security issues. The Mayor's Office of the CTO and Cyber Command are identifying best practices in areas threat prevention, incident management, they'll be shared as a resource for small businesses. Small Business Services intends to create free trainings to provide educational resources and information to

small businesses on methods to protect against threats and respond to breaches. Such training will be aligned with the best practices created by my office and Cyber Command. The city will continue its multiagency approach of partnering with industry to ensure that we attract effective and tailored technology tools that support New Yorkers and their businesses. We remain dedicated to helping New York City and its residents in dealing with the threat of cyber attacks. As President Kennedy said nearly 60 years ago, that challenge is one we are willing to accept. We appreciate the council's attention to this critical issue. My colleagues and I will be happy to answer your questions. Thank you.

CHAIRPERSON HOLDEN: Thank you. We've been joined by Council Member Yeger. Just, ah, I'll open, ah, and I'll pass it off to my co-chair. I just want to ask a few questions initially. This competition, so the security will be affordable for small businesses. You know, that's a relative term.

CHIEF TECHNOLOGY OFFICER FARMER: It sure is.

CHAIRPERSON HOLDEN: Um, for the smallest business will it be affordable, ah, I mean, 'cause,

you know, is there a number, is there a price, so that we can put out there?

CHIEF TECHNOLOGY OFFICER FARMER: Thank you for the question, Chair Holden. We looked at the numbers that you've looked at as well about the fact that most of these small- to medium-size businesses, most of these small businesses, are really micro businesses, as was noted by Chair Gjonaj. And so we're looking at businesses that have very few people, that have very small budgets, and don't have IT expertise. And specifically targeting those. And the solutions that, ah, came out of the challenge itself, ah, the three companies that ended up being awarded, um, the prizes, those are geared towards exactly that. So to your point that it's hard to give an exact number because the situation is different for different businesses and frankly the, the choices that individual businesses make might be different. But in the broader tool set, the set of tools that are out there that businesses could approach, we wanted to make sure that we were identifying and adding new tools that would help those micro businesses that have some of the smallest budgets and the least IT expertise on the staff.

CHAIRPERSON HOLDEN: So, so the three winners, they're creating, um, they're in competition so, so, ah, a small business can choose between the three or, um, is that, are multi layers also of security?

CHIEF TECHNOLOGY OFFICER FARMER: Sure.

CHAIRPERSON HOLDEN: So somebody could buy into, let's say, the lowest would have, you know, be least secure, but it's the cheapest, I guess?

CHIEF TECHNOLOGY OFFICER FARMER: That's a good question. So that's not exactly the approach that we took.

CHAIRPERSON HOLDEN: All right.

CHIEF TECHNOLOGY OFFICER FARMER: The three winners are actually different, so they're providing different tools that might needed by different businesses and different circumstances. We also are not saying that these are the only tools out there. In fact, by working with the Global Cyber Alliance and the Cyber Readiness Institute, um, we are putting these tools, highlighting them in context of other tools that exist out in the marketplace, some of which are available for free today and ensuring that, ah, small businesses here in New York

understand the different ways that these tools can be useful to them, ah, again, no matter what their budget is or what their level of IT expertise is.

CHAIRPERSON HOLDEN: OK. In doing your outreach to small businesses and, you know, I know my colleague, Mark Gjonaj, will ask some, some more questions on small businesses, but, um, what, just in doing the outreach did you, what did you find that, um, many of the small businesses in New York City, how are they being targeted? Like is it malware, ransom ware, what, what is, or unauthorized use? What did you see that most alarmed you?

CHIEF TECHNOLOGY OFFICER FARMER: Before I pass it over to my colleague from Cyber Command, ah, to speak from their perspective, in terms of the challenge itself we actually developed this challenge after hearing from small businesses. We surveyed hundreds of small businesses here in the city and heard from them what their, their challenges were and what their experiences had been. And so that's how we ended up with the challenge statement that we did, with the kinds of engagement, the kinds of workshops that we ran. In terms of, um, more specific details

around some of the cyber threats that are out there I'll pass it along to Quiessence.

QUIESSENCE PHILLIPS: Thank you for the question again. So I, I agree. I think, ah, some of the challenges are unique for small businesses simply because they are smaller. However, ah, the threats tend to be some of the same that enterprises also face. So, ah, obviously one of those being, ah, phishing, ah, spam emails, ah, what we call malicious spam where users would receive ah, a malicious link or, ah, a phishing link to provide information that could cause harm to that user or to that business. Other things that, ah, we see small businesses facing are, as you mentioned, ransom ware, ah, which is also delivered through some type of malspam or malicious spam emails. Ah, as I mentioned, as enterprises face, small businesses could face all of the same malicious type of threats, ah, it's really just about how they can respond to them and how we're equipping them to be able to respond.

CHAIRPERSON HOLDEN: OK. This one is for the Small Business Services, a question. Um, as you know, New York's Stop Hacks and Improved Electronics Data Security Act, I love this, otherwise known as

the SHIELD Act, um, will take effect very soon, in March, and will require businesses to implement appropriate cyber security safeguards. Many mom and pop shops are not even aware of the new regulations and may not even be aware of the, um, their establish, ah, their, their stores are at risk, um, for cyber attack. How does SBS, how is SBS informing small businesses about the new regulations?

ASSISTANT COMMISSIONER GIAMPIETRO: Business Cyber Security Act. And thank you again for the question.

CHAIRPERSON HOLDEN: All right.

ASSISTANT COMMISSIONER GIAMPIETRO: Can you hear me? So basically cyber, ah, cyber security is an integral component of business continuity. And as you know SBS, after Hurricane Sandy, and subsequent has been developing, you know, Councilman Gjonaj as well, a comprehensive webinar and workshop series. So we've, we've begun incorporating cyber and data security issues into our more broad, ah, business continuity and business resiliency efforts. As part of that, because of the SHIELD, as you know, and we're, again, focused on small businesses, so there's a distinction. I'm not a SHIELD expert.

However, there's a distinction between the larger enterprises as well as the smaller. So what we've done, to be, again, a perfect word that you had again and the point of being proactive is that we've incorporated, ah, targeting those businesses that are small and their requirements, um, the two primary, 'cause we want the information to be digestible for these businesses, um, so, um, there is a, there was, not a requirement but businesses as of October were encouraged to create data plans and, and put those in place. And in March we're informing businesses that there will be the requirement to inform clients if indeed there is a, a particular access or access to data and having those two pillars kind of reinforce to businesses as we again inevitably leveraged the guidance that will be coming from our partners. And, again, as we know, it's a complex, cyber security is a complex and ever-changing vehicle, so we want to ensure that our educational services are tailored to the respective parties, are standardized, and we are fortunate to have an extensive network of, ah, community-based organizations and LDCs, ah, where we can kind of impart this information citywide.

CHAIRPERSON HOLDEN: So you are organizing like seminars or...

ASSISTANT COMMISSIONER GIAMPIETRO: Actually, we have both.

CHAIRPERSON HOLDEN: Or training?

ASSISTANT COMMISSIONER GIAMPIETRO: We actually have, and we, what we've done, again to be proactive, ah, you know, create the best, um, efficacy for the SHIELD Act and general information, we already began incorporating, um, high-level information on the SHIELD Act into our webinars, which we have one tomorrow, as well as other items, like the plastic bag...

CHAIRPERSON HOLDEN: Where are these webinars, are they?

ASSISTANT COMMISSIONER GIAMPIETRO: The webinars are conducted from our offices and we work with our particular providers to encourage as many businesses. Ah, we're thinking of scaling these to train the trainers, so the LDCs and our business, ah, um, partners. Business organizational partners can also do the same. And we also want to amplify this, working with your offices as well.

CHAIRPERSON HOLDEN: Well that, see, that's the key because we have some communities that don't have LDCs....

ASSISTANT COMMISSIONER GIAMPIETRO: Exactly.

CHAIRPERSON HOLDEN: You know, and they, so the, they're on their own, many of these small businesses. So we need, we need some kind of outreach other than just, you know, putting out something on your website.

ASSISTANT COMMISSIONER GIAMPIETRO: And, and perfectly, and, ah, I don't want to monopolize this, ah, so, we also have a, our mobile bands and our small business advisors and client advisors that go specifically to businesses as needed and neighborhoods. So we're, we're very versatile in where we can target and, ah, have a have a broad, ah, [inaudible] broad map.

CHAIRPERSON HOLDEN: OK. Um, this is for the CTO a question. Last May your office issued a report called Truth in Broadband, Public Wi-Fi in New York City. According to this report, ah, your office would collect, ah, relevant agreements, um, for free

public Wi-Fi systems and post them on a website. Um, are these agreements, ah, collected and posted?

CHIEF TECHNOLOGY OFFICER FARMER: Thank you for the question, Council Member. Ah, the Truth in Broadband report that you referred to we think was an important, ah, marker along the way as we developed, as we did the research that allowed us to develop the New York City Internet Master Plan. Ah, this approach for how every New Yorker and every small businesses has connectivity at home, on the go, and in the workplace, really relevant to small businesses and, um, business districts in the outer boroughs. And so as we look at the need for public Wi-Fi, public spaces, um, we've been doing that research. It's not currently posted, um, beyond the initial report. We have a team of people that are working on subsequent reports and updating the website as we speak. So I would expect that in the future we'll have that information online.

CHAIRPERSON HOLDEN: Yeah, according to the report your office will develop uniform contract language based on recommended policies and standards to be used as a template for future Wi-Fi development.

CHIEF TECHNOLOGY OFFICER FARMER: Yup, and so as part of the best practices that, ah, our office in collaboration with Cyber Command and colleagues is developing around both access to connectivity and also cyber security and privacy around that connectivity. That's all wrapped up in the work that's being done.

CHAIRPERSON HOLDEN: Um, what is your opinion, um, well, let me just ask this question. During the briefing with our committee on public Wi-Fi last summer your colleague mentioned that your office will be working with the Office of Cyber Command to issue cyber security protocols applicable for public Wi-Fi. Um, what is, what's the progress in drafting these protocols? I don't know if you...

CHIEF TECHNOLOGY OFFICER FARMER: That's exactly right.

CHAIRPERSON HOLDEN: I know...

CHIEF TECHNOLOGY OFFICER FARMER: I think you're, we're thinking about the same things.

CHAIRPERSON HOLDEN: Yeah.

CHIEF TECHNOLOGY OFFICER FARMER: So I appreciate the question. These are, are the best practices that we are working on as we speak, um,

that we believe that the experience from the challenge and the experience of interacting with these 169 different proposals that came in and people behind them, the expertise behind them, as well as the expertise in, ah, the nonprofit community, places like Global Cyber Alliance and Cyber Readiness Institute, that's all informing this, this work that we're doing to develop these best practices.

CHAIRPERSON HOLDEN: Yeah, so when should we expect that, ah, the protocols?

CHIEF TECHNOLOGY OFFICER FARMER: We don't have an exact date for you but, ah, middle of this year I'd say.

CHAIRPERSON HOLDEN: Well, like President Kennedy had like the moonshot.

CHIEF TECHNOLOGY OFFICER FARMER: He did, he did. He said the [inaudible]...

CHAIRPERSON HOLDEN: [inaudible]

CHIEF TECHNOLOGY OFFICER FARMER: You know what, President Kennedy said at the end of the decade I can promise you...

CHAIRPERSON HOLDEN: Yeah, you're not saying end of the decade.

CHIEF TECHNOLOGY OFFICER FARMER: ...well before 2029.

CHAIRPERSON HOLDEN: All right.

CHIEF TECHNOLOGY OFFICER FARMER: Ah, we're, ah, we're targeting this summer.

CHAIRPERSON HOLDEN: All right.

QUIESSENCE PHILLIPS: What I can add to that, ah, as part of that initiative we have released, ah, what we have been referring to as the, the Quad9, which is available for the public Wi-Fi. So, ah, one thing that New York City Cyber Command has done is work with, ah, all of the places, especially, like for example public libraries, um, parks within or throughout New York City have, ah, initialized the Quad9, which provides the protection for, ah, residents that are on the Wi-Fi in those different places from being to access website that were intentionally, um, implemented for malicious purposes. So there has been some headway on that.

CHAIRPERSON HOLDEN: Um, I'll turn it over to my colleagues. I have a few more question, but, ah, Mark, Mark Gjonaj.

CHAIRPERSON GJONAJ: Thank you, Chair. Um, so in your, in your own words, in the most

simplest way we can describe this for those that are listening in today, how big of a threat is cyber security to our small businesses?

CHIEF TECHNOLOGY OFFICER FARMER: I'll, I'll just start it off before, ah, inviting my, my colleagues to chime in. Um, I think we're completely aligned with, um, with the folks in this room and the rationale for having this conversation today because we take it very seriously, and as life is increasingly lived online, as businesses increasingly connect with customers or potential customers online and, um, more data exists in our world, um, that means there's, there's, ah, there's simply more threats out there. And we are doing the work right now to make that better to address these challenges. But we also don't expect, ah, we're not under any illusion that the risks will go away. Ah, this is, this is the reality in which we live and we're very fortunate to have expertise of, of Cyber Command, um, and I think a lot of foresight went into the creation of Cyber Command a few years back, ah, because having the team that Quiessence is on is, ah, is an incredible asset to this city. And so I'll let others chime in.

QUIESSENCE PHILLIPS: Sure, I can provide a few examples with relationship to the threats, um, I know there was an earlier question around this as well. Um, so I think some of the things that, that small businesses are facing are, um, as I mentioned, phishing, um, emails, password compromises, denial of service attempts to those small businesses. So the risk is high. Ah, however, I would say that with the proper, um, protocols in place, with the proper cyber security and data security programs in place, small businesses can effectively respond and, ah, in most cases try to prevent as much as possible to reduce the risk to, to their companies.

CHAIRPERSON GJONAJ: Before you answer, sir, I just want to piggyback on that one question. According to the data that we have, 40% of online attacks are now aimed at small business. Do we agree with this information?

CHIEF TECHNOLOGY OFFICER FARMER: I haven't seen the exact numbers.

CHAIRPERSON GJONAJ: [inaudible]

CHIEF TECHNOLOGY OFFICER FARMER: But clearly there are a lot of small businesses and we expect that they would be, ah, under threat online.

CHAIRPERSON GJONAJ: Fourteen percent are prepared.

QUIESSENCE PHILLIPS: I, I'm familiar with the study. I believe that was released by our center.

CHAIRPERSON GJONAJ: And what the, and after hearing that startling fact, of the more than 200,000 businesses and only 14% of them are prepared for cyber attacks, 60% close within the first six months after a cyber attack. This is equivalent to a Hurricane Sandy, an earthquake of, ah, epic proportions. If we were to lose our small businesses this would not be New York City. Our neighborhoods and our communities wouldn't be what they area. The employment, the tax base, it's all under threat. And I'm looking at this number and I repeated it twice in my opening statement for, hopefully for an eyebrow to be raised. And I'm not hearing that, yeah, this is a, an unforeseeable future for our small businesses based on this study.

CHIEF TECHNOLOGY OFFICER FARMER: It sounds like Quiessence is familiar with this study. Ah, I am not familiar with that particular study.

But I will say this, which is that we agree that small businesses are the lifeblood of New York City.

CHAIRPERSON GJONAJ: Great.

CHIEF TECHNOLOGY OFFICER FARMER: And that our economy relies on their continued success. Um, and it's both, as you mentioned, ah, unthinkable that New York City would lose such a substantial number of its small businesses. In the 21st century there are risks that come along with the benefits of the tools that we use and it's our job, all of our jobs, to ensure that those benefits are maximized and those risks are minimized and mitigated. And so the work that we are doing is to ensure that small businesses have the tools that they need, have the expertise that they need, no matter how small they are. Ah, going back to the challenge statement, thinking about a small businesses and micro business could actually have access to the same kinds of tools that a Fortune 500 company has, ah, that's a big, that's, that's a hard thing to figure out. How do you actually level that playing field? Um, but it's one that we're making progress on. It's one that the challenges contributed to, but we also never imagined the challenge was a silver bullet. It was, it was

very much a way to accelerate our progress and we think it's done that. But we're continuing to work on this issue and we absolutely will because we recognize that all the things you said are true, that we need to ensure that the small businesses here in New York thrive. And are protected from the various harms that do exist in the world they operate in, in the year 2020.

ASSISTANT COMMISSIONER GIAMPIETRO: Just, just quickly to add is that, as you know, um, ah, with our educational tools and what we're hearing, gleaning, ah, small businesses, especially micro businesses, um, mom and pops, and it, it is an alarming statistic and, and how that's reflected in, in New York City. It's, ah, the education and awareness and, when businesses, as we all know, are faced with so many challenges and so many issues and small businesses are just trying to operate and get through the day and make the requisite amount of money and revenue to continue growing, ah, what we're finding and we're being proactive at SBS educational efforts and, again, and as we kind of infuse these with more information and guidance is to ensure businesses understand that this is as an important

issue as, as the others that they're facing. And, again, it's enveloping businesses with their requisite knowledge that's digestible, that's easy, that's accessible, to make action steps. Because we want to ensure that companies, what to do to avoid, what to do, um, if, if the event happens. And, ah, and that's what we're trying to do, that this amongst our business resiliency and business continuity efforts that we have, and, again, we've been focusing on areas of flooding, there's been, um, gas explosions, there's so many other items, as well as just running your business that this is now in the 21st century an integral part of running your business operations, to be secure in that.

CHAIRPERSON GJONAJ: So we all agree that, ah, this is a real threat. We all agree that this could have a tremendous impact on the city's, ah, future, the loss of small business using those statistics in that report. And there's a litmus test. How much money has been invested in your endeavors? See, I can only gauge this and this is why these hearings are so important, if we realize the threat is real and it's threatening the economy of the city, as well as we have a fidelity

responsibility and moral responsibility to protect our small businesses, how much money is it your budget allocated to protecting our small businesses? What budget do you have?

CHIEF TECHNOLOGY OFFICER FARMER: Well, I'll start off by saying it's, it's a hard question to answer because there are a number of different initiatives, ah, some of them not necessarily represented at this table today.

CHAIRPERSON GJONAJ: Well, let's talk about yours.

CHIEF TECHNOLOGY OFFICER FARMER: So the thing that we, the thing that my office, the Mayor's Office of the CTO, has done is this challenge, ah, working with our partners, dedicating budget, dedicating personnel to ensure that this is an area of focus for us, and so...

CHAIRPERSON GJONAJ: So how many people are working um, on this particular project?

CHIEF TECHNOLOGY OFFICER FARMER: It depends on how you define it. I would, a team, a team of, ah, five [inaudible] six people spend a lot of their time on this say. I'd say two of them, this

is their primary focus. Has been over the course of the past year plus.

CHAIRPERSON GJONAJ: Mr. Farmer, imminent threat, irreparable damage, and we have six people, two people full time.

CHIEF TECHNOLOGY OFFICER FARMER: Well, so that's, you asked about my team in particular.

CHAIRPERSON GJONAJ: Yeah.

CHIEF TECHNOLOGY OFFICER FARMER: I, I run a relatively small team when you think about the overall city. So I think it's worth looking at the size of Cyber Command, which has been built in recent years specifically to respond to the, the reality of, ah, the threats that exist today that didn't necessarily exist a few decades ago. And so a team of...

CHAIRPERSON GJONAJ: Right, but you've been, I'm sorry, your, this program began in 2018, I would imagine?

CHIEF TECHNOLOGY OFFICER FARMER: Right.

CHAIRPERSON GJONAJ: So now it's two years into the program.

CHIEF TECHNOLOGY OFFICER FARMER: It was the end of 2018, November, December.

CHAIRPERSON GJONAJ: Ah, a year and a half into this program, and we still have not, your team is, what you're proposing here, well, then, let's look at this way. Since to me it's all about, um, the money that we put towards this initiative. What were the awards that those three, ah, winners received.

CHIEF TECHNOLOGY OFFICER FARMER: The awards for the winners were, ah, $10,000 each.

CHAIRPERSON GJONAJ: So $30,000 was the, um, the price.

CHIEF TECHNOLOGY OFFICER FARMER: There was actually, the other finalists also received prizes, so it was $60,000 total.

CHAIRPERSON GJONAJ: And the New York City of 95 billion dollars we've invested $60,000 to bring in the, ah, think tanks of the world to engage in this competition.

CHIEF TECHNOLOGY OFFICER FARMER: So I, I hear you. And, um, I agree with the point that resources are part of what's required here. Part of what's required is resources. However, I want to point out that we received 169 responses. People knew what the size of the prize was here and the

reason to do this is not to win the $10,000, the reason is to, for the people who respond, either to solve a program they believe in, just personally in their own hearts, ah, or to gain business, ah, here in New York City. And so they view this challenge as an opportunity to launch a new customer base, ah, and that's what we believe has happened and will continue to happen. And so the challenge framework tries to use relatively small amounts of resources to actually have a big impact. That's the whole idea. Um, but I just want to be clear that that is one particular component of what the city has done and, and should not be viewed as the entirety or the totality of the city's...

CHAIRPERSON GJONAJ: But that's why these hearings are so important.

CHIEF TECHNOLOGY OFFICER FARMER: OK.

CHAIRPERSON GJONAJ: We look at each individual thing and compartment and step, and we analyze and figure out how to improve. But, ah, I'm encouraged by your words of there are people out there that want to do the right thing.

CHIEF TECHNOLOGY OFFICER FARMER: Um-hmm.

CHAIRPERSON GJONAJ: Um, there are also people out there that want to do the right thing that have full-time jobs and they have to provide for their families, and I couldn't get away that at home with my own wife and two kids and say, you know, let's do the right thing.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON GJONAJ: They want the bacon. They want the benefits of life and they want their bells and whistles. If we really wanted to make a challenge and bring the best of the best in and create this think tank, $10,000 is not going to get anyone too motivated. There are people that would do it for free. If the prize was much greater and the award, I would expect many more would compete, bringing in the best of the best, and if we realized how important this is to our future, the stability of our economy, the very essence of surviving of these small businesses, I think we have to put more money into it. And...

CHIEF TECHNOLOGY OFFICER FARMER: I am absolutely open to that conversation for sure.

CHAIRPERSON GJONAJ: Right.

CHIEF TECHNOLOGY OFFICER FARMER: Ah, I just don't want, and I think I've been pretty clear this, I don't anyone to think that that's the entirety. I don't want anyone to think that that is not, that that covers the work that is being done at Cyber Command.

CHAIRPERSON GJONAJ: We're gonna get to...

CHIEF TECHNOLOGY OFFICER FARMER: Or the work...

CHAIRPERSON GJONAJ: Right, we're gonna get to Cyber Command, but I'm talking about our particular initiative.

CHIEF TECHNOLOGY OFFICER FARMER: Sure, or, or the work being done, through, say, the EDC and their Cyber NYC program, a 100 million dollar program, so you get to grow jobs and skills in the cyber security industry right here in New York City. And so these are all complementary. Ah, and again, if there's, if there's an opportunity, ah, to discuss the right level of resources, we view the 169 respondents that we got as a good signal there's a lot of interest at the level at we went out previously, but, ah, open to discussions or ways to

test and figure out if there's another level of resources that shows us being good stewards of taxpayer dollars and maximizing impact in terms of the benefits that we create for New Yorkers and New York City businesses.

CHAIRPERSON GJONAJ: Music to my ears. I fight for every taxpayer dollar to make sure it's spent wisely. This would be a wise investment of taxpayer dollars.

CHIEF TECHNOLOGY OFFICER FARMER: That's good to hear. And we're happy to work with you on that.

CHAIRPERSON GJONAJ: Well, would, what would you assume, or what would you estimate the budget for your department and your initiative if you were in a perfect world, what that budget look like? What would that manpower look like? Given, given, as we stated, this, the concerns that were just raised?

CHIEF TECHNOLOGY OFFICER FARMER: I think it's, it's tough for me on the spot to come up with a number. I'm happy to think about that and, and get back to you, and it also depends on some of the other [inaudible].

CHAIRPERSON GJONAJ: Do you feel that you're adequately staffed? Do you feel that you have an adequate budget to meet your needs? I'm trying to get, I'm trying get, ah...

CHIEF TECHNOLOGY OFFICER FARMER: [inaudible] it depends on what the, it depends on what's being asked of the office. We're currently in the process of, ah, of getting to a place...

CHAIRPERSON GJONAJ: You have a responsibility.

CHIEF TECHNOLOGY OFFICER FARMER: ...where I feel that we can really deliver on all of the things that we're trying to do. Um, this is certainly an important part. But I think thinking about alternately what the context is, what, what the overall portfolio is, and understanding whether we have the resources, um, to maximize our impact.

CHAIRPERSON GJONAJ: You have a responsibility that you've taken on. It sounds like your, your heart and your head are in the right place to move this forward.

CHIEF TECHNOLOGY OFFICER FARMER: Thank you.

CHAIRPERSON GJONAJ: The way it works is collectively we come up with a budget. So this is your opportunity to say, hey, City Council, we want to, we want you and need you as a partner and we need X millions invested in this and here's the reason why. I'm waiting for you to say, hey...

CHIEF TECHNOLOGY OFFICER FARMER: I very much appreciate that and I, I, think...

CHAIRPERSON GJONAJ: Otherwise we have to assume that you're OK, that you're comfortable, that you're properly staffed, and that it's in good hands and we don't have to put any additional resources towards your responsibilities.

CHIEF TECHNOLOGY OFFICER FARMER: So I think there's two different things there.

CHAIRPERSON GJONAJ: OK.

CHIEF TECHNOLOGY OFFICER FARMER: One, we are staffed and I think we do have great talent and expertise that we've been able to bring in to city government that's doing a good job on behalf of New Yorkers. Whether or not the changing threat environment might require changes to our responses and, and various levels of resourcing, I think that's a conversation we should have. I, I am not in a

position right now to speak, ah, in response to your question, but I would be very happy to have that conversation.

CHAIRPERSON GJONAJ: OK. Well, the number of staff that you mentioned, by the way, for your responsibility?

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON GJONAJ: I have more staff that are doing constituent services. Full time.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON GJONAJ: Just to put things in comparison.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON GJONAJ: And, and they don't have, and constituent services are important.

CHIEF TECHNOLOGY OFFICER FARMER: Yep.

CHAIRPERSON GJONAJ: Ah, to make sure that the needs and we can help navigate through the government. This is a threat to the future of New York City and based on the numbers of two full time and four part-timers, ah, is not, for the responsibility that you have.

CHIEF TECHNOLOGY OFFICER FARMER: And I appreciate that. I just want...

CHAIRPERSON GJONAJ: Not what I was...

CHIEF TECHNOLOGY OFFICER FARMER: I just want to reiterate that we are working with partner agencies and so very much collaborating through the various agencies in the New York City government. So when you say how many people in New York City government are working on this issue, it far exceeds the number of my particular office [inaudible].

CHAIRPERSON GJONAJ: Who would be able to give us that information, from the dais? Who, who are you working with? If I wanted a snapshot...

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON GJONAJ: And the people listening to us here wanted a snapshot to actually hear what is being done, how many people, what's the total budget, what is really being done to get, to be as proactive as possible while we're educating and informing and building the infrastructure that's needed? Who can give us that answer?

CHIEF TECHNOLOGY OFFICER FARMER: Yeah. It's a good question and the challenge there is that there are people in all of these agencies and offices of New York City government who are focused on, on this issue. And the staffing levels varying, the

resources varies. Some agencies, um, might have very large numbers of people, and so we'd have to go do that diligence and research, ah, to come back to you with any kind of number and then that would then lead into a conversation on budget and how much time is being dedicated to this, and so it gets, it gets tricky, but to your point of let's, let's right size the resourcing to the threats, and I think that's a point well taken and one that, that we agree with.

CHAIRPERSON GJONAJ: Thank you. But that, that's the purpose of this hearing, so we understand exactly what's going on, a snapshot, and that's how we prepare for them, and based on these hearings we figure out what the next steps are.

CHIEF TECHNOLOGY OFFICER FARMER: Um-hmm.

CHAIRPERSON GJONAJ: Collectively. That's the reason we're here. So I hope that you can get back to us with an actual number. I'm sure my cochair and the rest of my colleagues would want to know, um, understanding what has come to light today.

CHIEF TECHNOLOGY OFFICER FARMER: Um-hmm.

CHAIRPERSON GJONAJ: Um, 60% of businesses were closed after a cyber attack. I don't think we can, any of us, can be the same after this

hearing if we truly care about the backbone of our economy. Maybe I can get more information from you and what you're doing to help shed some light on the resources that are at your disposal?

QUIESSENCE PHILLIPS: Sure, and thank you for the question. I would agree that, um, the threat is evolving and, ah, the problem, thus the, the resources are evolving. Ah, I think the administration has put forth great, ah, in support of Cyber Command for this effort and others regarding cyber security. Ah, to answer your question around, um, the budget, ah, for this fiscal year we have been awarded 94 million for, with 186 head count. I will be very transparent that that budget and that head count is not specifically for this initiative. However, ah, awareness and training in working with SBS and CTO's office is an integral part of New York City Cyber Command. So some of our resources, we have a dedicated group within New York City Cyber Command that works on awareness and training, thus in close collaboration with the CTO and SBS.

CHAIRPERSON GJONAJ: How many of the head count are actually working specifically on cyber security?

QUIESSENCE PHILLIPS: Everyone for cyber, in Cyber Command.

CHAIRPERSON GJONAJ: What that's, you have a budget of 184.

QUIESSENCE PHILLIPS: We have a budget of 94 million with 186 account for this fiscal year.

CHAIRPERSON GJONAJ: And the head count means they're employed or, because when we use the head count they're currently employed.

QUIESSENCE PHILLIPS: So I think currently employed I might be about 111.

CHAIRPERSON GJONAJ: So that's the real number.

QUIESSENCE PHILLIPS: Yes.

CHAIRPERSON GJONAJ: 111 people, not 186.

QUIESSENCE PHILLIPS: Correct.

CHAIRPERSON GJONAJ: OK. Do you feel that you are adequately budgeting yourself for the challenges that you have that allow you to operate and, ah, get ahead of this thing, this real threat?

QUIESSENCE PHILLIPS: At the moment I would say yes. I would also say, as I mentioned earlier, that the threat is evolving. The landscape is evolving. So that will change, ah, and we are

working closely with OMB and City Hall to make sure that as the landscape evolves, ah, and our capacity to take it on for the city, ah, those resources are accounted for and we're, we'll be represented accordingly.

CHAIRPERSON GJONAJ: You mentioned, what was the word before, ransom, cyber attack through ransom?

QUIESSENCE PHILLIPS: Ransom ware?

CHAIRPERSON GJONAJ: Ransom ware. I was a victim of that, by the way, on my personal computer.

QUIESSENCE PHILLIPS: OK, sorry to hear that.

CHAIRPERSON GJONAJ: And just for those of us, I found out the hard way what that was, and they take control of your computer and you get an email that says if you want your information back you have to pay X dollars.

QUIESSENCE PHILLIPS: Right.

CHAIRPERSON GJONAJ: And I understand that many people are forced to pay and never get that data anyhow, or it comes incomplete. Am I correct here? Your own experiences or what you've heard.

QUIESSENCE PHILLIPS: That is correct.

CHAIRPERSON GJONAJ: Isn't that insane, that we're not talking more about this and we're advising everyone out there this is what can happen to you? Small businesses, your livelihoods are in jeopardy and can be taken for ransom.

QUIESSENCE PHILLIPS: I do believe that there is a good amount of literature out there that speaks about ransom ware, um, that many organizations do provide for small businesses and, ah, as mentioned earlier we are working diligently with SBS to put forth, ah, best practices for small businesses so they can take this in consideration, and as, ah, John Paul Farmer mentioned with the moonshot challenge and other authorities, um, that can assist small businesses with software or, you know, just things that they could implement within their operation to ensure that this does not occur and if it does how to properly respond to it.

CHAIRPERSON GJONAJ: So the 200, over 200,000 businesses that exist, um, when you say we're out there and there are groups that are educating our small businesses. Walk me through that. Because

I've been a part of some of these educational programs and initiatives and how we get the word out.

QUIESSENCE PHILLIPS: Yeah, I think that would be probably be better answered by SBS with regard to...

CHAIRPERSON GJONAJ: No, as far as you're doing, so we have partners that actually educate and, I'll get to SBS, I'm saving the best for last.

QUIESSENCE PHILLIPS: OK [laughs]. So walking through how partners are actually educating the small businesses?

CHAIRPERSON GJONAJ: Um-hmm.

QUIESSENCE PHILLIPS: I think most, honestly, most of it is around like online literature.

CHAIRPERSON GJONAJ: Online?

QUIESSENCE PHILLIPS: Yes, um, and then others are, as mentioned earlier, workshops for small businesses, I know like there's the Global Cyber Alliance as well that offers, ah, software and best practices also that, ah, small businesses can use. Um, we also, with the New York City Cyber Command, um, NYC Secure Initiative, offer, as I mentioned earlier, Quad9 for public Wi-Fi, also offering NYC

Secure, which is our mobile app, ah, that allows small businesses to, ah, download onto their personal and business systems to ensure that they are aware of threats when they do occur and, ah, how to respond to them.

CHAIRPERSON GJONAJ: Ah, they download?

QUIESSENCE PHILLIPS: Yes, it's, it's an app that we developed called NYC Secure.

CHAIRPERSON GJONAJ: NYC Secure.

QUIESSENCE PHILLIPS: That's correct.

CHAIRPERSON GJONAJ: How many people have downloaded that app?

QUIESSENCE PHILLIPS: Ah, I have the number. Um, I believe we're about like 96,000.

CHAIRPERSON GJONAJ: 96,000 have downloaded, and when you say downloaded, these are small businesses or just downloads?

QUIESSENCE PHILLIPS: Residents, users, ah, of New York City.

CHAIRPERSON GJONAJ: OK, so there's a big difference...

QUIESSENCE PHILLIPS: Some of them, some of them including...

CHAIRPERSON GJONAJ: So if I'm trying to get a snapshot here of the 200,000 businesses, if 96,000 businesses downloaded this, now I'm saying OK, we're at 50% or 40% of the total small businesses. But how do we know of the 96,000, how many of those 200,000 businesses downloaded this information?

QUIESSENCE PHILLIPS: That's a fair question. I think we would have to go back and get you that answer.

CHAIRPERSON GJONAJ: That would be very important to know as we move forward.

QUIESSENCE PHILLIPS: Understood.

CHAIRPERSON GJONAJ: And I would, wouldn't be surprised if it's a fraction.

QUIESSENCE PHILLIPS: Fair enough.

CHAIRPERSON GJONAJ: Our small businesses are trying to survive. They're not even thinking of the threat of cyber security. And in online, um, where they don't have the freedom, the luxury, or the time, they're the first ones in and last ones out, ah, mindset, they're just trying to get through the end of the week and make sure they pay their bills. They're working 12 to 18 hour days. Come from that world. I hear it every day as the small business

chair that many of our small business owners don't even make minimum wage, where their employees, we value employees, where employees are making more than the employer. That's how competitive the world is out there. The world has changed before our very eyes. I would really love to have that number on how many small businesses downloaded this app, what more can be done if you are properly budgeted and funded for the responsibility that you have in assuring the viability and the future of the city. 8.6 million people with a 95 billion dollar budget, 94 million dollars with 111 people, taking on this major challenge, I don't know if that's enough. But I'm not the expert. You are. Thank you. Small Business Services. You, um, you have webinars, correct?

ASSISTANT COMMISSIONER GIAMPIETRO: Yep, and, and...

CHAIRPERSON GJONAJ: Elaborate, please.

ASSISTANT COMMISSIONER GIAMPIETRO: Yes, we have webinars and in addition in-person workshops. Ah, and that we, um, accelerated these. Again, we have, ah, had a comprehensive business continuity planning, again the genesis originally was, even pre-Sandy, you know, to ensure because we knew that there

were disruptions happening. You know, I think of even certain neighborhoods, which I'm not gonna mention now, that suffered in the, ah, one year a gas pipe explosion, a terrorist attack, and a variety of others, of, of just a power outage and, ah, and now we have been, we ensure that we triage and tailor. So that's what we do. We are, are consistent and methodical in the neighborhoods that we, ah, we go out to, we've incorporate, and we want to make sure there is equity of opportunity, that it's all neighborhoods, especially targeting those that are of, ah, smaller, um, business kind of clusters. And we've, and we've brought in, while waiting for the cyber security, but basically we know some of the, you know, the obvious steps to prevent and to respond if something happens and we've put those in, ah, into our trading efforts. So what we do is, like I said, we have the webinar, which is about an hour, a little bit over an hour, that's done multiple times during the month, typically twice. Ah, we, um, utilize the network or borough-wide, sometimes we'll focus on a borough or will respond to a council person's request, if indeed it's like in a particular area. And then we do the in-person workshops, which it's,

it's very similar information, and we want to make sure it's digestible because, as you know, ah, this could be overwhelming at times. You want to make sure that we keep it in a way that it's actionable for businesses. And we've noticed that there may be, um, you know, a shift, ah, and businesses are starting, because they may not have viewed this as like front and center issue when they're faced with so many others. So it's the kind of that psychology shift, like this is an issue and, again, we've done the webinars, we have one tomorrow, and the in-person workshops. And as we scale this up, ah, we want to have more of them. So they can be almost simultaneous.

CHAIRPERSON GJONAJ: So how many businesses have partaken in your seminars?

ASSISTANT COMMISSIONER GIAMPIETRO: I'd say over, Daniela, I'd say over in the past, one thousand participants.

CHAIRPERSON GJONAJ: One, is that small businesses or is that, oh, it's open to anybody?

ASSISTANT COMMISSIONER GIAMPIETRO: Ah, we target primarily small businesses.

CHAIRPERSON GJONAJ: But is it..

ASSISTANT COMMISSIONER GIAMPIETRO: It is, it is open to, um, businesses, but primarily small businesses through our outreach effort to small businesses, usually that's [inaudible].

CHAIRPERSON GJONAJ: So we're, we're going to make an assumption that there aren't, it's not a thousand small businesses. There are individuals that work or...

UNIDENTIFIED: [inaudible].

CHAIRPERSON GJONAJ: I'm sorry, ma'am?

UNIDENTIFIED: [inaudible].

CHAIRPERSON GJONAJ: Um-hmm. And in our best case scenario we know it's not a thousand but we'll assume that that could be the number, a thousand out of 220,000 businesses.

UNIDENTIFIED: [inaudible]

CHAIRPERSON HOLDEN: We're gonna have her, we've going to have you on the record.

ASSISTANT COMMISSIONER GIAMPIETRO: Um, basically, we'll get the exact number but...

CHAIRPERSON GJONAJ: My point being is that we are not doing...

ASSISTANT COMMISSIONER GIAMPIETRO: We, we have to scale it up.

CHAIRPERSON GJONAJ: ...we have to scale it up.

ASSISTANT COMMISSIONER GIAMPIETRO: We have to scale it up.

CHAIRPERSON GJONAJ: How many, so SBS, how many of your staff, of your full-time employees, are focused strictly on this, solely on this?

ASSISTANT COMMISSIONER GIAMPIETRO: Um-hmm, I would say because it's a, it's a hybrid approach, I would say in cyber security it's been business continuity generally, um, and with the client advertisers and climate advocates I would say that there's a, um, which is a broader because it's under the business, the, um, service division, ah, so on cyber security as part of business continuity and accessing and informing businesses there's at least, I'd say in our, in emergency response unit, about two dozen individuals that would be dedicated to ensuring business continuity and, and responding to the respective needs of businesses when they happen. Because this is, again, we're incorporating this into our general emergency response.

CHAIRPERSON GJONAJ: Right, but emergency response means something happens, then you react.

This is more educational, this is more proactive, it's completely different than...

ASSISTANT COMMISSIONER GIAMPIETRO: Exactly.

CHAIRPERSON GJONAJ: ...a response.

ASSISTANT COMMISSIONER GIAMPIETRO: Exactly. So the ER unit, unit, if you pulled that out I'd say there would be, um, again, I don't have the employee data, but of that team cyber security would be part of the information that would be delivered as we go forward, because as we're moving forward at least a dozen to 15, and I can get back to you on that issue.

CHAIRPERSON GJONAJ: All right. I don't want to take up more.

ASSISTANT COMMISSIONER GIAMPIETRO: No.

CHAIRPERSON GJONAJ: We, we need, we're definitely going to need more follow-up...

ASSISTANT COMMISSIONER GIAMPIETRO: Sure, sure.

CHAIRPERSON GJONAJ: ...with each of you respectively, um, and this is all about budget forming.

ASSISTANT COMMISSIONER GIAMPIETRO: Um-hmm, um-hmm.

CHAIRPERSON GJONAJ: If we're not putting the proper resources into it we're not going to optimize our abilities and take on these responsibilities that we have. This is real. The last, and my colleague brought up the New York State SHIELD Act, which takes effect March 21 of this year. In reading the outline, it's fewer than 50 employees. They have to have had less than 3 million in gross annual revenue in each of the last three fiscal years, and less than 5 million dollars in year-end total assets. If you're out, if you fall outside of that parameter I guess there is a different problem that you have. But small businesses must create a program under this SHIELD Act, which contains reasonable, it contains reasonable administrative, technical, physical safeguards that are incorporated. The size and complexity of the small businesses, the nature and scope of small business services, ah, activities, and the sensitivity of the personal information, the small business collects from or about consumers. That sounds like that's a whole a training and educational component in itself for

these small businesses. Just to comply. And what languages are we gonna do this in? When is going to be offered, and if it's online, given an opportunity to have small businesses partake, it's going to be a tremendous undertaking, tremendous.

CHIEF TECHNOLOGY OFFICER FARMER: Thank you for the question and bringing up, ah, the SHIELD Act. It's something that we are well acquainted with. It essentially has three components, one updating the definition of a data breach at the state level, um, two, requiring state entities and localities to be in, in sync with that new definition. And then, three, is what you're referring to, which is the requirement for data, ah, protection programs, and data security programs, I think it's how it's referred to. And small businesses under 50 have some, ah, of a lesser burden than larger businesses do, but still there's always the requirement for notifying customers, um, in the, in the event of a data breach. One of the things that we are seeing in the space of, um, small businesses and large businesses is a move towards more managed cloud-based services, so when you talk about the various things that will need to be done,

if those are being done by an intermediary service provider that that small business relies on, as opposed to the small business trying to do all themselves, then that could make that a much lighter lift for them, and that's a trend we've already been seeing in, in the business community, ah, and I would expect we'll see more of it. But to your point, um, we are working diligently understanding what the deadlines are to ensure that we are meeting all of those deadlines, doing everything that needs to be done, and ensuring that small businesses and everybody else who is subject to the SHIELD Act, um, is in, in compliance.

CHAIRPERSON GJONAJ: Thank you. Um, I'm going to give it back to my cochair.

CHAIRPERSON HOLDEN: OK.

CHAIRPERSON GJONAJ: If he can remember his questions that he left it.

CHAIRPERSON HOLDEN: No, I forgot all my questions.

CHAIRPERSON GJONAJ: Hey, I figured that.

CHAIRPERSON HOLDEN: Um, thank you. We've been joined by Council Member Paul Vallone, who is a, who is due to the Committee on Technology. So

welcome to Technology. OK. And, um, Council Member Perkins also joined us and Council Member Rosenthal was here and she might come back. We'll, we'll see, all right. Um, but I know Council Member Vallone has a question.

COUNCIL MEMBER VALLONE: Thank you to the chairs and thank you to Chair Holden for having me on the committee, very excited to be part of the committee and working with you Chair Gjonaj. Our districts are very similar in that we have the very same concerns and, and [inaudible] neighborhoods. This hearing is very important for the small businesses that we do host in our communities. And they are looking for this lifeline and for this information. So following on the chairs' questions, I just had a couple of follow-ups, because you touched on the grant process with the three $10,000 winners. You touched on the staffing of seven and then two are dedicated, um, I guess those are steps, just like with all committees, those are steps. What do you envision as the next step now after that grant process? What are we going to use with the winners? How are we going to integrate their ideas into our concerns?

CHIEF TECHNOLOGY OFFICER FARMER: Absolutely. Thank you for the question, Council Member. Ah, based on the process that we went through of this challenge, ah, we've learned a lot and we've created connections in this network, both with respondents to the challenge itself, but also with some of these third-party entities, like the Global Cyber Alliance, ah, and the Cyber Readiness Institute, that we continue to engage with, and those conversations, that expertise outside of government as well as the expertise we have inside government, Cyber Command and elsewhere, is informing the development of best practices, best practices specifically tailored to small businesses. So the challenge really focused on, ah, highlighting and identifying real live usable tools for small businesses to use. The best practices is broader. And so we mentioned earlier, and I don't know if you were in the room yet then, ah, we mentioned earlier that we're targeting the summer as when that deliverable, ah, will occur and we continue to work with our colleagues at Small Business Services about how that will be incorporated into their broader set of offerings for small businesses.

COUNCIL MEMBER VALLONE: Do you envision within those best practices the use or the contractual beginning of RFPs with some of those third-party providers, because obviously with the staff that you have you're not going to be the hub to provide that. We're gonna have to start alliances and contracts and working with the company's that are already providing that type of protection service to the small businesses. Will that be the next phase?

CHIEF TECHNOLOGY OFFICER FARMER: At, at this point we are not looking to be an intermediary. We're not looking to do contracting on behalf of small businesses. We're trying to bring, create a marketplace, essentially, where the small businesses and the various vendors, service providers that exist, ah, could connect with one another.

COUNCIL MEMBER VALLONE: So do you provide that in-service then? So I'm, I'm trying to think of how we can loop that all in.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

COUNCIL MEMBER VALLONE: So if I'm the small business that's, that is overwhelmed by this and threatened by these very real threats, how can we then connect you to that service to say, OK, you've

already vetted out and these are the five companies within the city, you know, restaurants have ABC service and rating and things, maybe there's a step that we can take that you can provide some of that vetting process.

CHIEF TECHNOLOGY OFFICER FARMER: So I think to the point of resourcing, vetting is, is time and resource intensive. And so what we did during the challenge was, was that. We did these technical assessments, um, various kinds of, of testing, working with small businesses to test in, ah, quote unquote real world environment to understand which of these really, ah, deserved to be highlighted. That isn't necessarily how my office is viewing our role going forward. We're really focused on that, what are the development, the development of best practices and then the marketplace aspect. In terms of us playing a role in the middle and being ah, ah, what's the word, a mega contractor or something of those sorts would actually...

COUNCIL MEMBER VALLONE: But even when you've...

CHIEF TECHNOLOGY OFFICER FARMER: ... dealing with procurements.

COUNCIL MEMBER VALLONE: ...discerned what the best practice is, what are we doing with that information? You already are putting yourself in that position. Once you determine the best practices you're already saying, OK, we've done this, we've done some, ah, vetting in some way, but we've also put this competition out and we're looking at and these are best practices at small businesses. You're already becoming that entity.

CHIEF TECHNOLOGY OFFICER FARMER: I would draw a line between best practices in general and specific tools and products being recommended or being the only ones available to small businesses. And so we want to make sure that there is a free and open competition.

COUNCIL MEMBER VALLONE: No, I, I hear you. I wouldn't think you would say there's always room for new technology.

CHIEF TECHNOLOGY OFFICER FARMER: Yep.

COUNCIL MEMBER VALLONE: So there's always gonna be a new, but I would think part of Chair Gjonaj's quest for additional resources would be, and maybe broadening or defining what your group is actually, can become, and make that the budgetary

ask. I, I think and I've seen it in so many other agencies, that we're just touching the tip of the iceberg here and in order to give what we need to fight for those resources to give you that. This might be the example. You don't have, clearly, the resource or the staffing power to take that next step. But I want you, I think you deserve to have that, and I think that's important because this is, this is now and this is what's gonna happen in the future, and we're gonna protect these small businesses, and if we're going to start to lay the groundwork in these areas, I think it's more intricate than what we're just touching today, and I would say, then my, my last two questions would be what interagency cooperation are you using now, because you're touching so many different, obviously, agencies, it's not just this hearing. Um, so what partners are you working with within other sister agencies, um, would be my last question.

CHIEF TECHNOLOGY OFFICER FARMER: I'll start off and then pass to my colleagues, because ultimately there are different networks at play here. Ah, we have focused through the last, over the last year and a half on working with Cyber Command and

Small Business Services and primarily the Economic Development Corporation around this particular, ah, set of efforts.

COUNCIL MEMBER VALLONE: So you're coming to my 1 o'clock hearing?

CHIEF TECHNOLOGY OFFICER FARMER: [laughs]

COUNCIL MEMBER VALLONE: So if [inaudible] EDC you should be at my 1 o'clock hearing.

CHIEF TECHNOLOGY OFFICER FARMER: [inaudible]. Um, but I'll pass it along to talk about the other networks that do exist as well.

QUIESSENCE PHILLIPS: I mean, for Cyber Command in general we partner with pretty much every agency in the city, ah, as our mission is to protect, defend, and respond to cyber threats in general for the City of New York, which is mostly for the systems that provide services to the businesses and the, the residents.

COUNCIL MEMBER VALLONE: So how are they getting you that data that you need?

QUIESSENCE PHILLIPS: What data in particular?

COUNCIL MEMBER VALLONE: Well, if you're working with every agency in the city to coordinate that, how, how are you processing, how are receiving that information? Do we have an annual report that is provided to you from each agency with regard to these topics? Are they just manually giving you information? I would tend to think we need some type of, ah, deadline as to when you get that to help you, say that each year, or every, whatever you need, six months, annual, I think we should put some, and the chairs then could put in a piece of legislation to help you on that, so that the agencies are giving you that information you need. Sometimes I'm just, I see that disconnect. Oh, I'm waiting for [inaudible] from DFTA but DFTA didn't get it to me 'cause they have seven staff members, ah, to handle that.

QUIESSENCE PHILLIPS: Understand, thank you for the question and comment. Um, I think compliance and auditing is, is, a huge part of, ah, Cyber Command's mission as well. Um, so this is not necessarily just for small businesses, but the larger organization. Ah, so part of that compliance effort is the reach out and working with agencies to collect a fair amount of information. We also have automated

ways to collect information that we use to somewhat build a, a risk posture and assessment of city agencies. Now, with regards to the small business front, in particular, ah, that's a little bit different, um, and that is more so, mostly in collaboration with CTO and SBS.

COUNCIL MEMBER VALLONE: It sounds like something we can explore.

QUIESSENCE PHILLIPS: Absolutely.

COUNCIL MEMBER VALLONE: I think there should be, um, ah, some mandatory reporting and indicators that Chair Holden and Chair Gjonaj could then have a hearing on an annual basis on that information and whether it's enough information, whether it's timely information, so that we're not reactionary but we're actually...

QUIESSENCE PHILLIPS: I appreciate.

COUNCIL MEMBER VALLONE: Looking forward to the next step.

QUIESSENCE PHILLIPS: I appreciate that and I think we would be happy to work with your office, too.

COUNCIL MEMBER VALLONE: Thank you to both chairs.

CHAIRPERSON HOLDEN: Thank you so much. Um, I just want, I want to ask a basic question here. Um, let's say a small business, or any business is, has an attack, a cyber attack. What do they do?

QUIESSENCE PHILLIPS: Is that a question for me?

CHAIRPERSON HOLDEN: They pick up the phone, they call 911? What do they do?

QUIESSENCE PHILLIPS: So I, I think, um, what we like to be, especially with the best practices, is to help the small businesses have somewhat of a cyber security program or incident response plan in place. However, what they would do today is get in contact with their law enforcement bodies.

CHAIRPERSON HOLDEN: So they would have to call 911 and say I've just been attacked, you know, on my, you know, my data has been breached.

CHIEF TECHNOLOGY OFFICER FARMER: If I can chime in, one other thing that small businesses can do and in many cases do do today is if they have a service provider, if they're working with, pick your big tech company, Google or Amazon or Microsoft, ah, they often will contact that company and that

company sometimes has resources that are available to customers like these small businesses to help solve the problem.

QUIESSENCE PHILLIPS: That's, that's very true, and as you may know that small businesses are very reliant on the third-parties that, you know, they, they integrate with, you know, some of those being Microsoft, which are larger companies. A lot of the small businesses being cloud-based or using cloud-based services can heavily rely on the third parties and they provide incident response services to them.

CHAIRPERSON HOLDEN: But on best practices, maybe it's their duty or the provider's duty to report this to the city and to your office, um, is that in place yet? Is that, I mean, I'd think that you'd want to know about it. I would think CTO should know, ah, Small Business Services should know, so we know how many attacks, we know where they're coming from, we know that they're focusing on this line of business. Maybe some businesses are more susceptible to attacks because of the structure. So is that in place now? So if I, I call my provider, what is my provider going to do? All right, they're

going to try to give me better service or try to fix the problem. However, you don't, your office doesn't know about it. Your office doesn't know about it. So should we require the businesses where data has been breached that they have to report this to the city?

CHIEF TECHNOLOGY OFFICER FARMER: I'm open to having a conversation. I think, ah, the rationale that you laid out about why that would be beneficial, clearly there's, there's some reasoning there, good reasoning. At the same time it is a requirement on small businesses, we want to make sure that, ah, we're, we're giving small businesses, um, we're asking things of small businesses that, that absolutely have value because of the reasons as Chair Gjonaj previously brought up, ah, the various demands on, on their time and attention and the lack of resources that [inaudible].

CHAIRPERSON HOLDEN: Yeah, 'cause we, we know some companies, larger companies, they didn't know they were attacked.

CHIEF TECHNOLOGY OFFICER FARMER: Sure.

CHAIRPERSON HOLDEN: Or if they did, they didn't report it to anybody for sometimes a year, a

year and a half, two years, or never reported it. And so we, we were compromised, the public, the customers were, so there should be a requirement.

CHIEF TECHNOLOGY OFFICER FARMER: The customer, ah, reporting requirement is part of the SHIELD Act.

CHAIRPERSON HOLDEN: Is part, is part of the SHIELD?

CHIEF TECHNOLOGY OFFICER FARMER: So that's part of it.

CHAIRPERSON HOLDEN: Yes.

CHIEF TECHNOLOGY OFFICER FARMER: I think what you're referring to, in terms of having to also report to the city...

CHAIRPERSON HOLDEN: I want, I want you guys...

CHIEF TECHNOLOGY OFFICER FARMER: ...in some capacity, some agency.

CHAIRPERSON HOLDEN: Yeah, as, as somebody who steers the ship I want you to know how many attacks are coming in and what kind, so you could be prepared.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON HOLDEN: So you could then, you know, notify, have another competition, say how do we beat this attack back? Or, you know, there's a lot, that, that information is very important to your office.

CHIEF TECHNOLOGY OFFICER FARMER: You're right.

CHAIRPERSON HOLDEN: But, but knowing how many attacks we've been hit with.

CHIEF TECHNOLOGY OFFICER FARMER: Having good data is the basis of..

CHAIRPERSON HOLDEN: Right.

CHIEF TECHNOLOGY OFFICER FARMER: ...of making good decisions, and so...

CHAIRPERSON HOLDEN: So in your opinion, if we required businesses, any businesses to report any cyber attack?

CHIEF TECHNOLOGY OFFICER FARMER: I think, ah, in terms of whether or not I'd be in favor of that it would depend on the details. So I would be happy to discuss that...

CHAIRPERSON HOLDEN: OK.

CHIEF TECHNOLOGY OFFICER FARMER: ...because I think, ah, a form of that would make a

lot of sense, but there are other forms of it that might be overreaching and so I think we would have to discuss the details.

CHAIRPERSON HOLDEN: How would it be overreaching, just to know that we were attacked and how data...

CHIEF TECHNOLOGY OFFICER FARMER: Well, how, well how, um, I'm just spit balling here, how quickly do they have to respond? They have to respond within an hour? They have to respond, ah, to 12 different agencies [inaudible] ...

CHAIRPERSON HOLDEN: No, no, I would say...

CHIEF TECHNOLOGY OFFICER FARMER: [inaudible] with six employees...

CHAIRPERSON HOLDEN: No, no, I would say one, 911 and 911 directs it to somebody's office, Cyber Command or your office, or Small Business, whatever.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah, and so those are the kinds of details that I think...

CHAIRPERSON HOLDEN: I know, but...

CHIEF TECHNOLOGY OFFICER FARMER: ...[inaudible] sit down and have [inaudible] discuss.

CHAIRPERSON HOLDEN: I know, but that would be beneficial, I think, to your office or anybody's office, the city, so that we could be prepared. How do we, how are we prepared if we don't, we didn't find out about it, we don't know. We don't how many attacks are, are coming or have been in the past, do we? We have no, no clue on how many attacks we've had.

CHIEF TECHNOLOGY OFFICER FARMER: And I think this is an important point that Quiessence has made is, is the evolving nature of the threat environment. So while historical data is useful, ah, it's not everything, because we know that this current year is going to be different from the last year. Ah, so, seeing what those trends are, and there are places to get a bunch of this data. There are private companies and, and researchers and think tanks who are looking at this generally, ah, and so understanding the trend lines is something that I think we are doing and Cyber Command in particular is doing already in terms of specific data that is New York, New York specific and, um, granular, not just survey level, because we have done surveys. Ah,

that's something that would be a step, a new step for us to take.

CHAIRPERSON HOLDEN: OK. So we'll, we'll talk about it, because I think, you know, in talking to the committee that we feel that we really need to know, we need more information on these cyber attacks and that protects the public. But I know the SHIELD Act doesn't, doesn't really, it's not specific and, and they're saying you, you put up a responsible safeguard. What does that mean? You know, I mean, I, I think your office could define responsible. Um, what's a, what's a protection that a small business should have, or any business should have to protect their, their information. The SHIELD Act is not specific on that, right?

CHIEF TECHNOLOGY OFFICER FARMER: I think that's right. There...

CHAIRPERSON HOLDEN: Right.

CHIEF TECHNOLOGY OFFICER FARMER: ...there needs to be, ah, some level of interpretation of what some of the terms they're used mean [inaudible].

CHAIRPERSON HOLDEN: So should we have our sent of guidelines in the city and, and not rely on the state?

CHIEF TECHNOLOGY OFFICER FARMER: Well, I, I, as you know, the SHIELD Act requires the city be in, in accord and sync with the state. Ah, there's, as far as I know, no limitation of potentially going further and having additional requirements. Ah, but that's the kind of thing that I think we would [inaudible].

CHAIRPERSON HOLDEN: But if you, did you critique, you look at it and say they're not doing enough, or maybe they're doing too much with the SHIELD Act? Have you looked into...?

CHIEF TECHNOLOGY OFFICER FARMER: I wouldn't say I looked at it with, with that particular eye.

CHAIRPERSON HOLDEN: OK, but you...

CHIEF TECHNOLOGY OFFICER FARMER: This came out right when I was coming onto the job.

CHAIRPERSON HOLDEN: OK.

CHIEF TECHNOLOGY OFFICER FARMER: And it was kind of already moving and it wasn't something that I really had [inaudible].

CHAIRPERSON HOLDEN: All right, but I, would like to hear some of your recommendations where we could improve upon it.

CHIEF TECHNOLOGY OFFICER FARMER: Sure.

CHAIRPERSON HOLDEN: And, um, protect us a little better in New York City.

CHIEF TECHNOLOGY OFFICER FARMER: OK.

CHAIRPERSON HOLDEN: Because we are a bigger target.

CHIEF TECHNOLOGY OFFICER FARMER: Absolutely.

CHAIRPERSON HOLDEN: We are the biggest target probably in the world.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON HOLDEN: So that we, we should be prepared. I just wanted to, one other question, which is a very general question about you, about your role in this whole subject matter here. Like as CTO what is your, how do you see yourself?

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON HOLDEN: Because it's kind of undefined, I think, to us out here.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON HOLDEN: Like where, where do you fit in to the big picture?

CHIEF TECHNOLOGY OFFICER FARMER: Sure, so, so the CTO role, as many of you know, was created

in 2014. I'm the third person to, ah, to sit in the role, and the way we are discussing this internally and externally is that we are looking at how improvements can be made in the future. There are so many of our colleges and peers throughout city government who are focused on today, ah, much like many of the small businesses, just doing the job, going through the work they have today. We have both the luxury and responsibility to work with them, collaborate with them on how improvements can be made in the future. And the future is not a distant thing for us. We're looking at how can we make improvements in the coming months. Ah, years and, and decades as well, but we're very much, we've got a bias towards the near future and getting things done quickly. Ah, there are four areas of focus for us at the moment. One is universal broadband, closing the digital divide once and for all, ensuring that every New Yorker and every New York City business has high-quality privacy-respecting connectivity. That's one area of focus. Digital inclusion is a big part of that, helping ensure that small business owners and older New Yorkers and young New Yorkers all understand both the benefits and the risks and can

take appropriate actions. So that is the universal broadband piece of the portfolio. The second piece is digital services. As more people are online, ensuring that we are delivering government services in a way that's user-centered, that meets New Yorkers where they are, whether that be on a smart phone, a laptop, a desktop at their business, ah meeting them where they are, making the kinds of transactions they need to do or the information they need to receive from government, easy and seamless and sensible. The third area of focus is innovation, and that's where the focus, ah, of the moonshot challenges reside. So the cyber security for small business moonshot challenge came out of our innovation work, where we apply innovation frameworks, ways of getting new ideas on the table quickly and then scaling them up, and that's what, ah, this lives out of. The other piece of that is co-labs where we work with neighborhoods. So innovation with agencies, innovation with communities. And the last area of focus is tech policy and digital rights. And I mentioned digital rights in my testimony because it's so foundational to what we do across the portfolio, ensuring that as we approach and address the new

technologies that are coming into the market, they are affecting the lives of New Yorkers and small businesses alike, that we ensure that we are looking at how we maximize benefit while minimizing and mitigating any potential risks or harms that could be created.

CHAIRPERSON HOLDEN: So the tech policy, um, that's where cyber, um, protection would come in, working with Cyber Command?

CHIEF TECHNOLOGY OFFICER FARMER: Yeah, it's, it's a combination of the digital rights...

CHAIRPERSON HOLDEN: Right.

CHIEF TECHNOLOGY OFFICER FARMER: ...and the tech policy and focus on cyber security, that's where...

CHAIRPERSON HOLDEN: But that's what I, I would like to, that's what I would like to discuss with you.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah.

CHAIRPERSON HOLDEN: As, as a legislator, that we could give you better protections, or at least better reporting from, from any business. Um, because I, you know, you have a lot to do. You have a lot of things going on. You have a lot of

catching, we as a city have a lot of catching up. Many cities have surpassed us in, in, in technology, at least in implementation. Um, so we have some catching up to do, but we also have, um, at least in the cyber, you know, the protection Cyber Command area, um, to, to stay ahead of the curve and that's something that, that's, I think has to be not only in your purview but the other, the other panelists, ah, their areas. So we're, we're at a stage here that, you know, what can we do as a City Council to make your job easier? Besides asking for more money or a better budget, you know. What, what else could we do? So we'd like to work with your office, my committee, and certainly small business, ah, services should, you know, will, you know, we'll try to work with you guys to, your office, to make your job a little easier. Because you've got a tough job.

CHIEF TECHNOLOGY OFFICER FARMER: Thank you, I appreciate those comments and, ah, and the question itself. I think the existence of this hearing is helpful. I think the facts that we know that this is a priority for the council and that is something that, that the administration has been working on, ah, and has been a priority for us is a

share priority. And so we should think through what that means. We should think through what that means in terms of resourcing, what that means in terms of future collaborations, what that means in terms of education to the various communities that we serve. Ah, and so I think, again, just the very existence of this is a helpful starting point for, I think, further collaboration and discussions. Ah, some of the specific questions that were brought up and the ideas that were proposed by the council here are, are very interesting and I think we want, I know I want to think through them and be able to discuss with some of my colleagues who have relevant expertise before weighing in definitively one way or the other, but generally we are open to any of these conversations in exploring how we protect New Yorkers, ah, in this age of, ah, cyber security not being a luxury but being simply a requirement, a fact of life, something that everybody, every individual and every small business needs to take into account.

CHAIRPERSON HOLDEN: Well, I'd like to, we, we mentioned, I think, at one of our meetings that we'd like to have some, um, round table in the future where we can discuss these kinds of things.

CHIEF TECHNOLOGY OFFICER FARMER: Yep.

CHAIRPERSON HOLDEN: So let's, let's work on that. Ah, my, my, ah, cochair wants to ask a couple more questions.

CHAIRPERSON GJONAJ: Yes, thank you, Council Member. Um, you're right sir. This is a good step in the right direction. It's my understanding, and I hope I'm not wrong here, but this may be the first hearing ever on cyber security aside from the hearing that allowed for Cyber Command to be formed, which was a bill. We've never had a hearing on understanding our vulnerabilities, um, what we, what we have in place and, ah, or ever discussed funding this type of initiative. So I have a couple of questions and I'll begin with SBS. How many small businesses have you assisted with cyber security-related questions?

ASSISTANT COMMISSIONER GIAMPIETRO: Cyber security-related questions? I'd say over, ah, I'd say close to, I'd like to get back to you on that.

CHAIRPERSON GJONAJ: OK.

ASSISTANT COMMISSIONER GIAMPIETRO: But it's well in, in the hundreds, ah, and again, like I

said, as a hybrid approach as part of the business continuity.

CHAIRPERSON GJONAJ: So how many people have called for a question on cyber security?

ASSISTANT COMMISSIONER GIAMPIETRO: [inaudible].

CHAIRPERSON GJONAJ: Or have...

ASSISTANT COMMISSIONER GIAMPIETRO: [inaudible] individually to the respective businesses, or we have group sessions and, and to the businesses and it's one of the key features. And, like I said, growing to be one of the more primary focal points.

CHAIRPERSON GJONAJ: Does anyone even know to call you?

ASSISTANT COMMISSIONER GIAMPIETRO: Pardon?

CHAIRPERSON GJONAJ: They wouldn't even know enough to call SBS under cyber security.

ASSISTANT COMMISSIONER GIAMPIETRO: They may not link that. They would go through a partner agency and then would be directed to us, and I believe because of business prep and the outgrowth of the Sandy initiative, um, business, business prep

has evolved to business continuity and business disruption. Um, so, um, Council Member, I believe through that we get the information. And then we go out directly to the businesses. And we have a mobile [inaudible].

CHAIRPERSON GJONAJ: All right, I'm glad you brought that up. So under preparedness, response, and recovery, right? Business emergency preparedness?

ASSISTANT COMMISSIONER GIAMPIETRO: Um-hmm.

CHAIRPERSON GJONAJ: Would you be surprised to learn that under SBS, your own category, there's no mention of cyber security?

ASSISTANT COMMISSIONER GIAMPIETRO: Um, I know that because it's considered, because we actually considered it as part of the umbrella of business continuity and I'm not, um, I'm not surprised, no, but it, it actually is, um, being, ah, infused, as I said, into all our literature and has been.

CHAIRPERSON GJONAJ: Well, it's not your website.

ASSISTANT COMMISSIONER GIAMPIETRO: It's not on the website.

CHAIRPERSON GJONAJ: Remember we talked about...

ASSISTANT COMMISSIONER GIAMPIETRO: Again...

CHAIRPERSON GJONAJ: ...an online presence...

ASSISTANT COMMISSIONER GIAMPIETRO: Yeah, yeah.

CHAIRPERSON GJONAJ: ...and if someone wanted to open up a business in New York City, if you are a resident and you now want to make the transformation from employee...

ASSISTANT COMMISSIONER GIAMPIETRO: Sure, sure, sure.

CHAIRPERSON GJONAJ: ...to save, your lifetime of savings, you're gonna make that final step and look, live the American dream.

ASSISTANT COMMISSIONER GIAMPIETRO: Because our...

CHAIRPERSON GJONAJ: And we rely on SBS as a guide, right? We pride ourselves that SBS, Small Business Services, are there to help you, guide

you in the right direction, make sure that you know about insurance and that you should have...

ASSISTANT COMMISSIONER GIAMPIETRO: Sure.

CHAIRPERSON GJONAJ: ...Worker' Comp and disability and we'll help you draft a lease and negotiate a lease. We do all these great things.

ASSISTANT COMMISSIONER GIAMPIETRO: As you know, yeah.

CHAIRPERSON GJONAJ: But yet cyber security is nowhere to be mentioned.

ASSISTANT COMMISSIONER GIAMPIETRO: Well, two things. A, um, you know, our, our web-based content is not static and it's always evolving and all those have been added. And, two, it is a growing effort and we want to ensure that what we have is smart, correct, and is present and current. We're not, we're not just going to wait for the best practices because our current best practices. So what we've done is already, as I, I'm using the term infused, we've gone out to the communities to bring the information directly to the businesses and our web site, that evolves and, again, is not static, and well, we constantly incorporate the new...

CHAIRPERSON GJONAJ: I know, but this is a little different. So if you're telling me, it's a little different from it. If you're telling me you're out there and with the limited resources that you have on education, right? And I'd like to see some of the literature now. Because now I, and this is why I get a little defensive. Online is where we're guiding most people to seek out services. And if we're informing our small businesses or future small businesses what you should know, that means if you want to open a bar and sell alcohol you need a liquor license, right? Now we give out the, we itemize step by step all the rules, the requirements that you should know.

ASSISTANT COMMISSIONER GIAMPIETRO: Yep.

CHAIRPERSON GJONAJ: We offer, ah, services. We'll come and visit your site before you open up to make sure that you're not in violation. Here's the 6000 rules and regulations, if you're an attorney you'll find them, if you're not an attorney good luck, in different languages. And we just talked about how potentially harming and damaging this is to New York City and those small businesses, and I'm hearing fluff now, my dear friend, on why

it's not mentioned online. And that you're giving out literature. It would be a lot, I would hope that we're going to have something online...

ASSISTANT COMMISSIONER GIAMPIETRO: Oh, definitely, definitely, definitely.

CHAIRPERSON GJONAJ: ...quickly, quickly.

ASSISTANT COMMISSIONER GIAMPIETRO: Definitely.

CHAIRPERSON GJONAJ: And save trees, forget about paper.

ASSISTANT COMMISSIONER GIAMPIETRO: And, like I said, we go out to the people themselves and talk in detail. But great, yes, and we're constantly evolving. Wonderful point.

CHAIRPERSON GJONAJ: So let me get back to the SHIELD Act, all right? So it says here, and I'm just going to read. This is why it's a little concerning for me and I'm glad that you brought this up, Chairman. Any person or business which owns or licenses computerized data, which includes private information, shall disclose any breach of the security of the system following discovering, following discovery, or notification of the breach in the security of the system to any resident of New

York State whose private information was or is reasonably believed to have been accessed or acquired by a person without valid authorization. That in itself is an explanation I can't even decipher. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the integrity of the system. That takes effect March 21. Less than a month from now.

ASSISTANT COMMISSIONER GIAMPIETRO: Um-hmm.

CHAIRPERSON GJONAJ: Are we ready?

CHIEF TECHNOLOGY OFFICER FARMER: We are working, the folks you see here, along with colleagues who are not here, ah, to meet that deadline and we're working diligently and anticipate that we will. So what you've mentioned is the expanded definition of breaches that affect residents of New York City.

CHAIRPERSON GJONAJ: Um-hmm.

CHIEF TECHNOLOGY OFFICER FARMER: Not just breaches that occur in New York City, and so that's part of the, what the SHIELD Act did was

expanding that definition, um, and then to the point of the, the timing, obviously following but without, without unreasonable delay and I think that's where we're gonna figure out what, what exactly that means. What is reasonable, what's unreasonable. Those are the kind of things.

CHAIRPERSON GJONAJ: So [inaudible] some experience, right? Are you familiar with the plastic ban and the tax base?

CHIEF TECHNOLOGY OFFICER FARMER: Um-hmm.

CHAIRPERSON GJONAJ: It's been [inaudible] and talked about for a number of years.

CHIEF TECHNOLOGY OFFICER FARMER: Yep.

CHAIRPERSON GJONAJ: Finally we have a deadline, and I have everyone up in arms saying we're not ready. You know how much advertisement, how much education, how much promotion has been done about this at a local level and a state level, and our businesses are not ready, let alone our consumers. That's plastic bags. And it's created such an uproar. This is much more devastating. March 21 is around the corner, and I'm not getting that sense that we're ready. We're working, I get it. We've been working on the plastic bag tax for years and

we're not ready. I really do believe we're behind and this hearing I would hope you would articulate how behind we are, what needs to be done to bring us up to speed so we can inform the general public of their responsibilities, articulate our responsibilities, and how we're going to meet these challenges together.

CHIEF TECHNOLOGY OFFICER FARMER: Um-hmm. I appreciate your question and the concern that you do have. I would, ah, not agree that we are behind.

CHAIRPERSON GJONAJ: OK.

CHIEF TECHNOLOGY OFFICER FARMER: Ah, we're working to meet the deadlines. And, as was brought up earlier in terms of the effect on small businesses, ah, the SHIELD Act has fewer requirements for small businesses than it does for large businesses, so we know that. And in addition our understanding of the number of small businesses that are working with third parties, many of those third parties, many of those third parties are already, um, functioning in a way that, that is likely to be in compliance with the SHIELD Act. So that's not...

CHAIRPERSON GJONAJ: Fourteen percent of small businesses are ready, in the report that we read, that we're familiar with.

CHIEF TECHNOLOGY OFFICER FARMER: Which report? So I'm, oh, are you talking about the [inaudible] report that, that you two knew about?

CHAIRPERSON GJONAJ: What's Intersect?

CHIEF TECHNOLOGY OFFICER FARMER: Ah, 14% are...

CHAIRPERSON GJONAJ: Are prepared for cyber security, they aren't aware of a cyber security threat.

CHIEF TECHNOLOGY OFFICER FARMER: So I...

CHAIRPERSON GJONAJ: I shouldn't have taken a proactive approach.

CHIEF TECHNOLOGY OFFICER FARMER: I shouldn't opine on a report I haven't read. However, I would think that that probably doesn't take into the number of small businesses that are working with large third-party tech companies that have many more resources and, and are prepared. I'm guessing that doesn't take that into account, because 14% sounds like it doesn't.

CHAIRPERSON GJONAJ: It sounds like you're more familiar with this report. As far as you are aware of?

QUIESSENCE PHILLIPS: I, I think I would probably agree with that, that most of the small businesses are working with larger organizations as third parties that are prepared for that. So while they're not prepared and maybe don't have proper response plans in place, ah, if they knew to make the proper call, which I can't state that they do, then they wouldn't be dead in the water, if you will.

COUNCIL MEMBER PERKINS: [inaudible]

CHAIRPERSON GJONAJ: Would you put on your microphone, Council Member.

COUNCIL MEMBER PERKINS: [inaudible].

CHIEF TECHNOLOGY OFFICER FARMER: thank you for the question, ah, Council Member Perkins. This is something that we are discussing earlier, the, the two tracks that most small businesses take today and we recommend to them, one being law enforcement. If there is a crime that's been committed, ah, then that’s an appropriate thing to do. And the other is if they have a third-party service provider, ah, and that platform is having

issues, um, so then they would call that, that third party. And in many cases those third parties have substantial, um, not just IT, but cyber security resources in house that they make available to solve problems for their customers. So while the small business itself, in many cases such as a micro business with six or eight or 10 employees wouldn't have the IT and cyber security expertise on staff, they might be able to access it through these companies with which they work, these, these vendors essentially.

COUNCIL MEMBER PERKINS: In the feedback from the [inaudible] to measure whether that they are [inaudible]?

CHIEF TECHNOLOGY OFFICER FARMER: During the course of the moonshot challenge on cyber security for small businesses, that's not something that we directly tried to assess. We, we try to understand the current state of how small businesses are operating and ask them for what their needs were, and that's what led us in the direction that we went in, but we didn't go in trying to get data on what percentage of companies are taking that route and what percentage of companies are satisfied

specifically with that route of working with vendors and getting, getting kind of a backup from them.

COUNCIL MEMBER PERKINS: [inaudible] thank you.

CHIEF TECHNOLOGY OFFICER FARMER: You're welcome.

CHAIRPERSON GJONAJ: Um, this is for CTO. How in your opinion can business protect their communications on the websites? Do, I mean, we're trying to educate now and have an understanding. What is that, what is that you suggest they do to protect communications? Let alone data?

CHIEF TECHNOLOGY OFFICER FARMER: Sure. So the question you're asking about communications, are you thinking email? Are you thinking...

CHAIRPERSON GJONAJ: Emails.

CHIEF TECHNOLOGY OFFICER FARMER: ...forms? What's the, is there a?

CHAIRPERSON GJONAJ: All of the above.

CHIEF TECHNOLOGY OFFICER FARMER: All the above. Um, I think these are the kinds of questions that we were looking to address through the best practices that are being developed. It's too early for me to say specifically here are the three things

exactly they should do. Ah, but there are, there are good practices that are out there. An, when you look at, I've mentioned Global Cyber Alliance, for instance. They have a toolkit that is specifically tailored to small businesses. Now it's of the tailored to New York City small businesses, it's not necessarily tailored to the various, ah, rules and just realities of working in New York City, but it is tailored to small businesses that are unlikely to have significant resources on staff, and so those things exist today and those are the kind of things that are informing the process, ah, that we're going through.

CHAIRPERSON GJONAJ: [inaudible]

QUIESSENCE PHILLIPS: I could elaborate on that.

CHAIRPERSON GJONAJ: Please.

QUIESSENCE PHILLIPS: Um, I would say that this is not necessarily geared towards email communication only, but there are a few strategies that small businesses can use and many of them do use. Um, whereas taking into consideration, you know, the assets that they do have, um, ensuring that they have stronger passwords, ensuring that they

incorporate multifactorial identification to ensure that if those if those...

CHAIRPERSON GJONAJ: Those are terms, by the way, that most of our mom and pop shops have no idea what you just said.

QUIESSENCE PHILLIPS: I absolutely agree with that, and I think that's where the best practices come into play so we are, one, explaining terminology and then also explaining how they can incorporate that into preventative and protective measures and then also providing assistance on response and what could be done.

CHAIRPERSON GJONAJ: And that, and that holds for those that speak English. Could you imagine the ones that don't even, that English is their second language?

QUIESSENCE PHILLIPS: I can imagine, yeah, I think...

CHAIRPERSON GJONAJ: The challenges that they're faced with, and are we offering any of those in any other language, any information that we have on cyber security in other language? Do you even have personnel that speak in other languages that can answer a question of, of, Hispanic or Albanian or

Pakistani or Indian, or anyone that doesn't speak English?

QUIESSENCE PHILLIPS: From a, from a Cyber Command perspective, ah, for the app that we did release, New City Cyber Command or NYC Secure, we released that app with, I believe, 13 different languages. Ah, so we have taken that into consideration. Obviously, New York City is a multicultural, ah, so we shouldn't release anything really without taking into consideration other languages.

CHAIRPERSON GJONAJ: And what about CTO?

CHIEF TECHNOLOGY OFFICER FARMER: Absolutely, this is actually an issue that I appreciate you bring up, because it's one I'm very passionate about. We recognize that 49% of all households in New York speak a language other than English at home.

CHAIRPERSON GJONAJ: Um-hmm.

CHIEF TECHNOLOGY OFFICER FARMER: Literally hundreds of different languages are spoken here. And so when we think about the services and the information we provide, we'd make sure that that is provided in a way that's useable to the broad

swath of, of people who create what is New York City. And so in terms of staff, yes, we do have a number of different languages spoken on my particular team but that's not enough because it's never going to be all of the languages spoken. So I, and this is veering off a bit from the conversation here today. I'd be happy to continue it more. Um, I would very much like to take a holistic approach to how we incorporate technology and human beings to create maximum benefit and the maximum number of, ah, languages that can be translated into, ah, in terms of not just, ah, the content that we're trying to reach small businesses with, but also all of the various information services that the city provides.

CHAIRPERSON GJONAJ: Do you have a plan or recommendation on what steps a business should take in case of a cyber attack or a breach?

CHIEF TECHNOLOGY OFFICER FARMER: So I think we're coming back a bit to some of the...

CHAIRPERSON GJONAJ: Um-hmm, I am, because I'm going to circle back to SBS and then.

CHIEF TECHNOLOGY OFFICER FARMER: Sure, so, um, in terms of a specific here's what to do that doesn't exist today in a way that's...

CHAIRPERSON GJONAJ: Give me a [inaudible] are you suggesting [inaudible] 911?

CHIEF TECHNOLOGY OFFICER FARMER: ...endorsed by the city?

CHAIRPERSON GJONAJ: Are you suggesting call 911?

CHIEF TECHNOLOGY OFFICER FARMER: If they believe a crime has been committed, then yes.

CHAIRPERSON GJONAJ: And if we, if we to call 911...

CHIEF TECHNOLOGY OFFICER FARMER: If they believe a crime has been and New York City is the appropriate law enforcement jurisdiction, just to clarify.

CHAIRPERSON GJONAJ: Well, if I own a pizzeria and my computer system has been hacked or it's been held under ransom, or anything, or I just realized that someone penetrated my limited security.

CHIEF TECHNOLOGY OFFICER FARMER: Yeah. I, I expect in most cases it's exactly what you said.

CHAIRPERSON GJONAJ: What should I do?

CHIEF TECHNOLOGY OFFICER FARMER: What should you do? If you believe a crime has been committed I would suggest that you reach out to law

enforcement. If you believe that New York City is the appropriate level of law enforcement and jurisdiction then I would say 911 makes sense. If...

CHAIRPERSON GJONAJ: So help me out here. I'm trying to, I really ask a straightforward question. I am a small business owner, a pizzeria, my system has just been broken into. Who should I call? You say if New York City is the proper...

CHIEF TECHNOLOGY OFFICER FARMER: Sure, so, why, I think we need a little more information than my system has been broken into. What you makes you think your system has been broken into? Can you access your system, or can you access it however you believe somebody else is also accessing it? So those kinds of question I think need to be, to be answered, and then understanding the, ah, urgency and the immediacy of, of the need. Again, can you not access your information, as you mentioned your own experience with ransom ware unfortunately, ah, where that's one kind of experience.

CHAIRPERSON GJONAJ: So what should you do in the ransom? What should be done by that small business?

CHIEF TECHNOLOGY OFFICER FARMER: Um, I think on ransom ware as a specific note is that something that Cyber Command has specific, ah, responses to, or is it, is it just part of the general, how you it, how would you respond?

QUIESSENCE PHILLIPS: I think for a small business in particular would still fall in line with any other type of threat. I know there a fair amount of small businesses that are reaching out to law enforcement, especially because law enforcement does work on the cyber-enabled crime, which a lot of small businesses are facing. Ah, so ransom ware would fall into general cyber security issues or incidents that a small business would face. Obviously, the impact could be devastating, but it would still fall into that category.

CHAIRPERSON GJONAJ: And if we follow through, a call has been made. Now New York, NYPD officer shows up, I would imagine. What, how long does that take? What happens then? Do they take the computer? Do they come with technicians to help you understand what has happened? Walk us through. People, it's not, it's not the people in the audience here. We have, this is being televised and they're

gonna want to know, right, this could happen to me. And I should know. Help us inform New Yorkers. What happens at that point, or are you not even aware?

QUIESSENCE PHILLIPS: So I, I don't want to speak on behalf of law enforcement, um, but I think what we could also mention here is some of the steps that are taken with the third party, ah, that we, where we spoke about earlier that there's an internet service provider or another cloud provider where, ah, a small business can reach out to that body as well to receive assistance.

CHAIRPERSON GJONAJ: But NYPD reporting, or 911, we just walked through that. What are, what should happen next if we're even aware of what could happen next?

QUIESSENCE PHILLIPS: It should be connecting that small business with a party that could assist with incident response.

CHAIRPERSON GJONAJ: Which would?

QUIESSENCE PHILLIPS: If, and, and that can vary, right, depending on the type of attack. Also depending on the third party that could be involved. So I can't give you a prescription at the moment just because it, it varies based on the type

of attack that could occur. It also depends on, you know, whether data was siphoned, whether there was monetary loss. You know, there's a wide array, array of incidents that could occur, thus different response procedures that could occur.

CHAIRPERSON GJONAJ: You see how far we are?

QUIESSENCE PHILLIPS: I do.

CHAIRPERSON GJONAJ: And I'm a legislator, I'm having a hard time following this, let alone someone that could be hacked right this very moment? And I'm just wondering what they would do besides grab their hair and say oh my God, you know, my business now is under jeopardy and I don't even know enough to report it and who to report it to and what to expect? Do I touch the computer? Do I not touch the computer? Is it evidence now, is it part of a crime scene? These are real life questions that people don't even know.

QUIESSENCE PHILLIPS: Absolutely. And I...

CHAIRPERSON GJONAJ: And we're not, we're not creating a dialogue and maybe we should do a test and maybe this is what you should be doing. What

happens if a 911 call is made? How, how long does it take for a response? How many people are dedicated to responding? Do they come dressed in, men and women in blue uniforms, ah, as a traditional NYPD? How do we know what they do after that? I mean, this is all important information as we inform, we understand our responsibilities, and we help shape the future and how we respond, and it doesn't seem like we really know what happens.

QUIESSENCE PHILLIPS: I understand. I understand your point, absolutely. I think...

CHAIRPERSON GJONAJ: What would you like to see? How about that? What, in a perfect world, because that's how we get to something, what would you like to see occur once that phone call is made? And that may be helpful in determining head counts and budgeting and everything else?

CHIEF TECHNOLOGY OFFICER FARMER: So I, I think we're moving a bit beyond the conversations that we've been having previously, which were much more about what, what should be done, in what circumstances, and we're, we're discussing who should be involved. And, ah, I think it's an important conversation to have but it's not necessarily one

that we have been focused on over the course of the last year plus. That's really been much more focused on the what, what should be done, and, ah, the who, and then that gets into the question of resources, 'cause the who has been resourced to do the thing, um, there can be a variety of different perspectives on that, and so I, I'm hesitant for us to share our own personal perspectives without going through the process with our colleagues who have their own expertise, ah, to understand what we think would really be the best approach.

QUIESSENCE PHILLIPS: I think it's just important to highlight that a lot of work that we've been doing thus far is around prevention as well, and equipping the small businesses to understand the risk of cyber security and what could be do, could be done. Um, with respect to your question they've been, the, the most recent questions are focus on response, which is a whole 'nother category.

CHAIRPERSON GJONAJ: I'm trying to figure this all out.

QUIESSENCE PHILLIPS: Absolutely, and I respect that. Um, so I think what we can do is, you know, discuss internally, I think we would be happy

to have further discussions with the, with the council on response mechanisms as well, and I think this would go into the best practices that we are looking to release.

CHAIRPERSON GJONAJ: SBS, do you want to answer that?

ASSISTANT COMMISSIONER GIAMPIETRO: Well, again, like I said, we are, ah, we're going to leverage and continue as we're working forward in building out, ah, the cyber and data security aspect of our efforts. Ah, and we want to make sure that this is robust. We do, ah, again, as I said, we have it divided into, at a high level, three different, one is, ah, three different areas. One is [inaudible] prevent, um, what happens and like what resources might be available, and then, ah, basic steps on what to do in the instance, which is law enforcement, um, and that, and also can we look at immediately, can you continue to operate? Is there an alternative way to go back, maybe become a Luddite and go back to paper. There's some mechanism that you continue operations, 'cause that's where our focus has always been. Three, even prior to the SHIELD Act, do you have a plan in place? We even

tell people this, you know, just generally, to notify your businesses or, ah, those, your employees, so there's a notification scale, you know, done. Just high level. Ah, and then, you know, you would step back before you respond to ransom ware, if you're being held ransom. Perhaps, um, I'm, I'm not an expert on this and it might be in the, ah, the best practices, but there may be, um, other services in the government, federal government, where they have already kind of broken ransom, um, certain types of common, um, phishing emails, and they may be able to help. So those would perhaps potentially be involved, ah, incorporated. So at a very high level we inform, ah, and again, to ensure businesses know that there are some options, and further options [inaudible]. In a way it's digestible as well and we try to make sure it's translated into the appropriate language.

CHIEF TECHNOLOGY OFFICER FARMER: And I would just, to, to wrap up this part of the conversation, I would just say, ah, I think Quiessence brought up a really important point, which is that threat prevention is plan A. That's plan A. How do we help small businesses here in New York City

avoid the threats? But we recognize that that isn't something that we can count on a hundred percent of the time and that's why we do need to have, ah, focus on incident response as well.

CHAIRPERSON GJONAJ: Thank you. So let's move onto another topic. Ah, cyber security insurance, um, is one of the ways to negate the financial risk associated with cyber attack, however, such policies are often confusing to non-experts. Does SBS have a, or plan to have a program to assist small businesses in making the right choices with regards to cyber security insurance? And then I'll follow up with CTO and then.

CHIEF TECHNOLOGY OFFICER FARMER: Certainly.

ASSISTANT COMMISSIONER GIAMPIETRO: As I said we're looking at all our, all our resources that we have and looking to see, because many businesses are small and the respective issues may be common but specific to, ah, again, particular issues that may or may not involve insurance. So we're looking at all the broad issues, all, all the resources, we want to basically even discuss this particularly one with council and our partners. But, again, we're looking

at all the broad resources now to see what the best way to respond is. We're learning to see what, um, actually is bubbling up is, ah, the needs of businesses right now.

CHAIRPERSON GJONAJ: Could you envision SBS playing a role in helping, um, negotiate cyber security insurance on behalf of, let's say, micro businesses or small business across the board?

ASSISTANT COMMISSIONER GIAMPIETRO: Um-hmm.

CHAIRPERSON GJONAJ: Um, going through the policy, negotiating it, negotiating the charges, and I can't even imagine what the fee would be for such insurance. I would imagine it depends on the number of terminals, the number of computers...

ASSISTANT COMMISSIONER GIAMPIETRO: Sure.

CHAIRPERSON GJONAJ: ...the type of information. It's very complicated stuff.

ASSISTANT COMMISSIONER GIAMPIETRO: And, again, I'm not an expert, particularly on insurance, and it is highly complex, insurance in general, um, from Sandy and going forward. What I would, ah, say is that I would take this back to the leadership at SBS and to like view this is part of the, kind of,

ah, is part of like its holistic approach right now. So that's what I would say. I would definitely, this would be potentially a resource that we'd look at.

CHAIRPERSON GJONAJ: So having the advantage of negotiating on behalf of 220,000 or 230,000 small businesses would probably ensure, um, the lowest premium possible, and put it into, ah, into those premiums and policies certain conditions, which you're more than capable of negotiating, including compliance with the SHIELD Act and the other issues that come was it. Which can then require periodic inspections to make sure that you are in compliance and updating. We're looking at different issues here, requirements, loss of data, which means loss of business, and then legislatively what are the fines if you don't comply? We can put, in trying to keep them in business we can put them out of business, which would be a new approach to New York City's, ah, heavy-handed policies and unfunded mandates. But we have to be mindful.

ASSISTANT COMMISSIONER GIAMPIETRO: Um-hmm. And, and I'll take this back to our agency leadership, this idea.

CHAIRPERSON GJONAJ: CTO, anything you want to add on cyber security insurance? What is your, ah?

CHIEF TECHNOLOGY OFFICER FARMER: Thanks for the question. Certainly it's a, it's a topic that's in discussion these days, not just here in New York City but, but elsewhere, and cyber security insurance is a, a potential tool. Ah, it's not one that we know is right for everyone. It's not necessarily a silver bullet, but it's one that we are exploring, looking at and considering where it might be appropriate. I think one of the things that is, um, implied in the question is, is not just is cyber security insurance effective, and, again, say, say you identify a [inaudible] case of small business for which it would be effective. There's the added question about that user experience. Does that small business owner understand what they're signing and what they're getting into, and are they able to do the risk analysis, the cost-benefit analysis. And so these are all questions that are being explored. It's a, it's potentially a tool of one of many, ah, that we would look at for New York City small businesses.

CHAIRPERSON GJONAJ: I don't want to get, I'm going ask you to, I don't want to get too far ahead of this, but we have requirements now for insurance. If you drive a car you must have insurance. If you have employees you need Workman's Comp and disability insurance, right? These things currently exist for the betterment of society and as a whole. Based on what I've heard today this is something that we should be looking into.

CHIEF TECHNOLOGY OFFICER FARMER: So it's not something that we have a firm position on, and again, as I mentioned, we're exploring as part of what we're doing week by week, ah, across the various agencies to develop these best practices and better inform, um, New York City about what, what tools are available. Ah, one of the, the potential differences with cyber security insurance versus, say, ah, flood insurance or earthquakes or hurricanes or all those things is the, the distributions are potentially more difficult to model and less normal. Ah, so less predictable. And so therefore the cost of the insurance in some cases, again, I'm not passing judgment on the entire industry, but one of the concerns that has been voiced by some critics is that

the cost of the insurance could outweigh the benefit and then especially if you have a small business owner who signed a contract with some fine print that they didn't fully understand, ah, that might actually very much flip it from being a good deal to a bad deal. Because those are the kinds of things that we're, we're getting into.

CHAIRPERSON GJONAJ: That's why I put it back on SBS. They can negotiate policies and terms and premiums and they're equipped to do so. They do it now. We offer, we offer these services across the board when it comes to small business. Yes, is it complicated? Absolutely. But this is complicated stuff we're talking about. And the future, ah, depends on our next step. Not only from compliance, but from actual, um, assuring that we, um, are prepared. So this is, ah, incredible. Ah, I feel that we're behind because I'm not getting the answers that I'm looking for. We don't even know how, what directions to give our small businesses. Um, and what they should expect from the moment they realize they were attacked and, ah, what they can do to prevent it and the education and outreach that's needed and the preparedness for them and their

awareness. I, it's, it's a tremendous undertaken, and what I heard so far is I don't think we've committed the right resources, the head counts, ah, prioritized this to the level that and the attention that it actually deserves, and I say that only from what I've read and heard so far.

CHIEF TECHNOLOGY OFFICER FARMER: I appreciate your focus on this and your concern, because it's a concern that we share. I would say that we have dedicated head count. We have dedicated resources. The question of whether they are the right levels is one that's a discussion we're happy to have. Um, but, ah, I don't want to minimize in any way the attention that the administration is placing on cyber security generally and generally cyber security for small businesses specifically.

CHAIRPERSON GJONAJ: I understand. It's a difficult position to defend. Did you want to add to that?

QUIESSENCE PHILLIPS: I don't have too much to add. I would just say that while the cyber security landscape evolving so is the, ah, cyber insurance landscape. I think we've learned a lot over the past years where it has been available. Ah,

to Mr. Farmer's points, um, sometimes the costs may outweigh the benefits for certain entities. I think it also depends on, um, the stance of the small business, whether they house much internally or they're, they're completely reliant on third-party services, ah, who then do have some type of power or authority to make change or notify or provide services in regards to incident response. So it's, to your point, it's very complicated. But, you know, it needs to be completely decoupled and guidance needs to be provided to the small businesses.

CHAIRPERSON GJONAJ: Do you see a role that credit cards can play, credit card companies or a surcharge that could be added that perhaps can create general fund that could provide this insurance to all small businesses, or micro businesses in particular, which we know that they're not prepared nor do they have the resources or wherewithal? Is there something in play that we could look at that could help build the resources, the funding that's needed to provide insurance across the board?

CHIEF TECHNOLOGY OFFICER FARMER: In terms of the question of funding and revenues and where they could come from to fund this, that's not

something that I think the people at this table today, ah, have focused on or necessarily would be our particular role in the administration.

CHAIRPERSON GJONAJ: SBS? We encourage cooperance. We encourage, ah, businesses coming together to buy products and services at a, negotiating based on share members so they can benefit from bulk purchase discount. Why should this be looked at any differently?

ASSISTANT COMMISSIONER GIAMPIETRO: Well, again, I haven't, um, actually delved into this myself. Ah, it, it is a, you know, a discussion point that you're bringing up and I'm not, I'm not prepared at this juncture right now because I'd want to ensure that I, you know, would bring it back to leadership and that I'm, we'd think about, you know, these efforts collectively as part of all of, um, the various, ah, mechanisms. But it's, you know, and I appreciate you stating that.

CHAIRPERSON GJONAJ: Thank you, Chairman. Chairman, I, ah, leave it to you.

CHAIRPERSON HOLDEN: Yes, I'm sorry, I had to run across the street. I have another committee meeting and it was on an important topic,

the BQE, and, um, something I've taken for 50 years of my life so I think I had to jump. But, anyway, it's raining out, so I just to make people are. You can see, I didn't have an umbrella. So, um, anyway, I'm back and I want to thank the panel, um, thanks for holding down the fort, my cochair, um, I hope he wasn't too hard on you when I was gone, but I know Mark Gjonaj has, is, really advocates for small businesses and has been doing that for quite some time, and I want to thank him and the committee for the input, and thank you for your testimony. Thank you all. Um, I've think we've come a long way, at least in learning about the cyber attacks and cyber technology, and I think we have some, some thing to cover. Um, however, I think if have, if we schedule a round table soon I think we might be able to, to approach some of the, the concerns, at least, ah, in terms of, um, legislation that we might be able to help you with. So, ah, I appreciate you, you all for, for testifying and, um, we're gonna call the next panel. Ah, we have one more panel. Anybody else want to, to testify, ah, can sign up at the desk over here. Thank you, thanks. Our, our next, our panel, our second panel, Derek Shanahan, Daniel

Golansy, and Steven Bellerin. The place cleared out, didn't it? Um, OK, who wants to start? Just state your name [inaudible] go ahead.

DANIEL GOLANSY: Sure. My name is Daniel Golansy and I am the CEO of a company called Atacama. Should I continue? I'm the CEO of a company called Atacama. We're a cyber security company here, based in New York City, and we are actually, we were one of the finalists of the moonshot challenge. I had prepared some testimony on paper, which of course I'll leave with the group, but given what I've heard over the past two hours, I think I should probably put this aside and speak more directly to some of the issues that the city faces. Ah, what we're dealing with here is crime. And just as we have, as the city dealt with crime for many, many years, so too are we now dealing with another type of crime. But there's a problem and, ah, I would encourage the City Council to think about this structurally in a very different way. So historically crime, it was specific in nature. It, it consisted of discrete events. Someone would rob your house. You would call the police department. They would come to your house and it was a who, a what, a where, a why, a when. There

was a criminal justice system that was equipped to deal with these sorts of events and they were relatively static in nature, insofar as the nature of robbing a house didn't change all that much over the course of what, two, three hundred years, right? Now we're dealing with something very different. We're dealing with a type of crime that is no longer static in nature. Ah, even the tools that we used to mitigate, ah, the, the effect of crime. So we used to use insurance. Somebody would rob your store and had insurance. And that insurance would compensate you for the loss of inventory and perhaps the loss of profits. Yes, we have cyber insurance. But that type of insurance can never put the cat back in the bag once personally identifying information is released. It cannot do it. It does not make sense for someone to call 911 in the event of a cyber attack. Our police department was not designed for that. Our criminal justice system was not designed to address these sorts of issues. So it would be folly for us to try to address them with the same framework. Now, if I were to come here and say, OK, the best thing to do would be this sort of regulation and I would tell you here's a proposal for the sort,

the sort of regulation we need. Maybe it's akin to the SHIELD Act. I could stand up here and say that, and that would be something probably you've hear frequently from people who provide testimony before you. Right? That's one possibility. I could do that. I could also say, you know what, we need a specific city agency, we need to provide a huge budget for that. You've heard that before as well, nothing new. If I said we need to negotiate bulk discounts on cyber insurance it would be a conventional sort of recommendation. Nothing all that new. I'm not going to recommend any of that. In fact, what I'm going to recommend is completely different and perhaps maybe a little bit unpopular, ah, but it will not cost the city a dime and it will not require a single page of new regulation. And when I discussed this with my colleagues yesterday one of them said to me, Dan, your testimony will not be popular because you're not recommending anyone spend any money or any new regulation. So let's see how this goes. Our city has 200 plus thousand small businesses per what I've heard earlier today. I don't know the exact number, but I believe it. What I will tell you is that to the best of my knowledge

there are 300,000-plus jobs related to the technology sector in New York City, 9000-plus start-ups, and large tech companies. If the city were to create a privately funded initiative, if the city were to create a not-for-profit that specifically addressed these issues, you would see tremendous participation from the private sector, from start-ups like my company, from some of the majors, who would step in and say, look, we have the expertise to help. Right now you have a forest fire that's burning hundreds of thousands of acres. And unfortunately the best tools that we can come up is a fire hose, is a, a garden hose. You'll never put the fire out. The structure of the problem does not lend itself to conventional solutions. It does not lend itself to conventional legislation. It does not lend itself to conventional budgeting processes. You need to think differential about this. If you were to create such a group you would have tremendous participation. And let me explain why. The free open source software community, which is one significant community within the software industry, has a lot of, a lot of motivation to do good work to demonstrate their prowess, to, ah, show how competent they are at

solving problems, so you have motivated actors who want to solve a problem, not purely for altruistic purposes, but for reputational purposes. They want to do it, they want to show how good they are. Plus, you have good-natured people who want to solve a problem. Dual motivation. Plus you have access to tremendous technical resources, people who are trained in this. So I'm not here to ask for money or legislation. I'm here to ask for leadership. I'm here to ask that the City Council establish a group, a privately funded group, and I'll put my money where my mouth is. Atacama, we're a start-up here in New York City. I'm from New York. I'm a proud New Yorker, right, I grew up in Queens. Lived here almost my whole life. And my, my company is a proud New York company and we will do our part. So I'm here to say we'll offer 10,000 free licenses to our software for small businesses should you establish such a group. And that's the beginning. We would go further than that, and I can assure you that others would also follow our lead if you were to do this. So that's a summary of what I had written here, and let me leave it there and see if you have any questions.

UNIDENTIFIED: [inaudible]

DANIEL GOLANSY: I've, ah, handed it to the...

CHAIRPERSON HOLDEN: Yeah, we have, we have a copy.

DANIEL GOLANSY: Handed it to your colleagues.

CHAIRPERSON HOLDEN: We have it. Thank you. I'll have some questions, but we'll go on to the next person. Then we'll ask questions.

STEVEN BELLAVIN: I'm Steven Bellavin, a professional of computer science of Columbia University [inaudible] law faculty, but I'm from Brooklyn originally, so [inaudible].

CHAIRPERSON HOLDEN: [inaudible] that's good.

STEVEN BELLAVIN: But, yeah, I, I grew up in Brooklyn, educated in the New York City public school system. I learned to program more than 50 years ago in a New York City high school. Ah, my first paid job was doing computer stuff at the municipal building, ah, right across the park. And I want to focus not on specialized tools, but on good cyber hygiene. A lot of the tools are like the

statins and blood pressure drugs and angiocardiograms and MRIs and all the other fancy high-tech stuff. I want to teach people how to exercise properly and eat properly. And there are, you know, I have very specific technical suggestions in my written testimony, which you have and anyone watching this on the web it's already on my website. There are, ah, a very few things that will go a very low way to preventing problems that hit small and even large businesses and to be able to recover. The first is good system administration, including especially regular backups. If you don't have backups you will not recover from ransom ware, recover from other types of breaches. It will be very much harder. I think that's a very large part of why we have this very high failure rate after hacks. People don't have good backups, made with an eye towards dealing with ransom ware. The second very important thing is to stay up to date on patches. All the major vendors try to make it very easy for you to install patches. Most breaches happen because businesses and individuals don't apply patches. And that includes things as large as the Equifax breach. There were many more things that went into that one. But the

root cause, the first penetration came because some website they operated did not install a patch for a known vulnerability. I cannot stress this too much. This is actually recommendation number one. And that comes down to good system administration. I recommend that the city university, the two-year colleagues and the four-year colleagues, establish curricula in system administration. I think that these curricula should include student, ah, staffed clinics to go out to the small businesses. It's not as simple as floss properly or brush your teeth properly. Every business is going to be a little bit different in terms of information flow, what it gathers, what it needs to do. But, you know, with a reasonable amount of training students can guide you in how to set this thing up, set this up and do it properly. Ah, the third thing is for any online services - banking, financial management, bookkeeping, and email - get away from simple passwords, use what's called two-factor authentication. Something as simple as this, literally USB key, quantity range, ranging from $20 to $50, depending on what brand you buy, supported by all major browsers, all major operating systems at

this point, will largely prevent successful phishing attacks, and this is where the big cause of email compromise and bank account compromise. Small business bank accounts are a huge, huge target for attackers because more money than the average consumer has and less recourse from, ah, from the banks. Other specific suggestions I have go to hearing a lot about recovery, that recovery, incident response and recovery is a much more specialized thing. You need referrals, you need resources. The city should make this available to small businesses. A loaner program for equipment. If you've been hacked while your own equipment is being imaged for law enforcement use, if that is what is desired, cleansed, reinstall from backups, get you back on the air with, say, a 30-day loan of a couple of computers, to let you get back on the air from your backups while you get your own equipment cleansed, rehabilitated, and put back into service. Again, that specialized and you need to see what went wrong to find out how you got hacked in the first place. These are comparatively low-cost programs and with system administration curricula at the colleagues, this is a great job opportunity to do everything from

two-year degree, I've, I've done it with a Ph.D., I know a lot of Ph.D. system administrators can go a very long way. But it can also work this is a huge job opportunity. Ah, the IT staff you talk about for the medium and large businesses, these are system administrators. These are great job opportunities and there's a shortage of this. So it would work educationally. It would also work to help the small businesses of this city. You've also heard about cyber insurance. One of the problems there is we do not have good actuarial data. It's very hard to say how, you know, what the premiums should be if you don't good have actuarial data. Every business is a little bit different. It's hard to have checklists that really apply, along the lines of the electrical code, which came out of the fire insurance industry. We don't, we're not at that level yet in the, ah, cyber security world beyond the basics like take backups, install patches, use multifactorial authentication. Ah, we need more data. I've been working at the national level to try to get more, get enough data to help researchers and regulators say what to do. I'll stop for now, but there's very

detailed technical recommendations in my written testimony.

CHAIRPERSON GJONAJ: Thank you, thank you so much.

DEREK SHANAHAN: Good afternoon. Thank you for having me and it's a pleasure to share, um, this time with you and very passionate panelists. My name is Derek with Paladin Cyber, on the leadership team here and, um, we were one of the three winners of the moonshot competition. So please to serendipitously be here for a cyber insurance conference, which I'm now going to after this even. So thank you for having me. Um, in a nutshell, Paladin Cyber is a cyber security start-up on a mission to make cyber resiliency practical for small businesses. So the reason why we were founded originally three years ago is exactly why we're all here today. And I'll expand on that. Cyber risk is increasing across the board. Um, technology is interwoven into nearly every business operation, whether it be large or small, enterprise or micro. Unfortunately, and very relevant to this conversation, most small businesses owners have not had the tools, know-how, or time to implement even

basic defense. So while most people think of highly sophisticated technical attacks when they hear cyber security, the biggest driver of cyber risk for small businesses is social engineering. Now, what social engineering is by definition is getting people to perform unauthorized action or divulge sensitive information. Now, most of the data breaches, ransom ware attacks and other cyber incidents you're hearing about involving phishing, the most common form of social engineering, um, as a part of the method of entry. Now, while cyber security often feels complex, let's simplify things, as we really need to play a game of telephone through different agencies, all the way to the smallest businesses in New York City. You can build a good foundation by incorporating four main components. Number one is awareness. Number two is prevention. Three is response, and then, as the worst form of risk control is insurance. So unawareness, the first step is really just instilling a security mindset. Now, businesses need to help their employees understand how to identify and properly handle the types of dangerous things they're bound to see in their inboxes and browsers. So PDFs, force-fed compliance

sessions, these are things that do not breed awareness by any means. Now, engaging with individuals through active conversation, interactive trainings and simulated attacks along the lines of phishing, that helps instill the right mindset and reduces the chance of human error through shock therapy, an actually meaningful interaction. Now, the second step here is prevention. Since we all know that human error is inevitable, I make mistakes every day, it's also important to implement active defenses to keep users and data safe. So this includes a toolbox to automatically detect and block malicious content, like ransom ware and phishing at the inbox level. And also browsers and on systems before they cause damage. So preventative risk measures are critical. Now with that said the best defenses fail and most small businesses wouldn't know where to begin if they were to hit, be hit by a cyber breach or privacy incident, which we talked about earlier during the first session. So this is both, both costly and confusing a process to undergo. Thankfully a core feature of cyber insurance, which will be the last bullet point, will address this very problem. So you look at things like computer

forensics, reputational risk, general disaster recovery, outreach to customers. That metric that was thrown out earlier about being out of business within six months of a cyber attack is very real, and I would say it's in some cases conservative of a number. And then lastly if you ask any cyber security expert they'll tell you that best defenses can fail and that's why cyber insurance exists, much like anything else out there. So the cyber insurance is a key component in building cyber resilience as there will always be a non-zero chance that your best efforts fail you, simple as that. The right insurance policy will not only help businesses recover quickly, but also cover the potential devastating cost of an incident in very simplified terms. You might see insurance polices out there that are hundreds of pages long with exclusions and nuances. Um, in the best-case scenario and the best market providers you'll see something distilled into 15 pages with intentionally broad coverage. So since there is no solution to address all four of these competencies for small businesses in one fell swoop, what we've done at Paladin Cyber is built an AI-enabled cyber platform, so this is something that can

be implemented for small businesses and enterprise businesses alike with zero IT expertise, zero hardware whatsoever, and we've partnered with Argo Insurance, who's based right down the street in Chelsea, to launch Cyber Sphere and Cyber Sphere was a core reason, in my opinion, of why we're able to win, or jointly win, the moonshot competition. This is a cyber protection solution offering small businesses, excuse me, easy-to-use security tools with a least a million dollars of cyber liability insurance. The, the average cyber breach, by many counts, and you'll read 10 different numbers, if you look at 10 different reports, I, I promise you that, ah, conservatively it's, it's in the minimum in the six figures. And for a small business that's unsustainable and untenable to actually weather it. So it costs less than, in most cases, about a thousand bucks a year for our policy. We try to keep it intentionally simple and intentionally priced at a, at a reasonable amount so that's a no brainer, just like your car insurance. So although this is a big uphill battle, small businesses can win the fight against this ubiquitous cyber crime, and we look

forward to continue to help the City of New York in this very defense. Thanks.

CHAIRPERSON GJONAJ: Um, thank you all. This is, ah, I, I wish the administration stayed around, ah, to listen to this. Um, 'cause some of the testimony, it sounds simple. Um, some, testimony of, if you get insurance, you, your prevention is very, very important, like you said. Um, yet, um, I'm not sure the administration is getting that in the way of outreach. I like the idea that you won, you won the competition, ah one of three winners. Um, I wasn't quite sure from their testimony what happens next. Did they tell you what happens next?

DEREK SHANAHAN: Sure, so...

CHAIRPERSON HOLDEN: I mean, they give you a stamp or, a whole, a ribbon, to put on?

DEREK SHANAHAN: It's hanging up in our office. Ah...

CHAIRPERSON HOLDEN: Yeah, and...

DEREK SHANAHAN: ...it's on our website, too, which is great, it's fantastic.

CHAIRPERSON HOLDEN: Right, but what happens now?

DEREK SHANAHAN: So there was a nominal prize, um, which is something that, that wasn't our, our sole mission, obviously. We wanted to evangelize across New York, given our insurance partner is in New York, and actually as of this morning we were trying to schedule time with the Small Business Administration through, ah, through the office of the CTO. So it was, it was a very appropriate room about an hour ago and unfortunately people had to leave. Um, but we're working on next steps now for distribution.

CHAIRPERSON HOLDEN: So you, they scheduled a meeting and then it was only an hour, and you don't know, you don't know the next step?

DEREK SHANAHAN: There is a bit of lag time after, the competition itself was in August here in New York and we found out, ah, about our victory around the end of the year, and then we've since picked up the conversation probably around four weeks ago, for next steps.

CHAIRPERSON HOLDEN: You mean government moves slowly?

DEREK SHANAHAN: Could have fooled me, I don't know.

CHAIRPERSON HOLDEN: You know, this is, well, this is alarming. I don't, I don't like it. I like the idea of the competition.

DEREK SHANAHAN: Yeah.

CHAIRPERSON HOLDEN: I don't know why they couldn't get started right as well as in September and have this ready to go. But I don't know, I still don't know the next step. Like, are they gonna promote the winners? Are they, are they going to, um, put you in touch with, you know, business associations? Are they doing that?

DEREK SHANAHAN: Well, the benefit of the, the State of New York is that it operates in a free trade zone and there are far less regulations to crawl through from the prospective of an insurance carrier, an insurance market. So in an ideal world we'd be able to give direct account to the 200,000 small businesses and get them some sort of loose, loose indication of what they would have to pay for a million dollars of cyber liability with all of the tools that we have attached for free. But we don't have the distribution strategy yet.

CHAIRPERSON HOLDEN: OK, so, but that's what, and then contracts haven't been talked about or anything like that?

DEREK SHANAHAN: That's right. Our, our program is live, but contractually with the State of New York nothing has been set in stone.

CHAIRPERSON HOLDEN: So in the time since August, um, many businesses have been attacked, unnecessarily, because if they had your software they might have been, it might have been blocked, right, and protected.

DEREK SHANAHAN: Ideally.

UNIDENTIFIED: Yup.

CHAIRPERSON HOLDEN: So we should, as legislators, push the administration to get moving. And we heard today that they're, they're going to work on it, they're working on it. But many of their proposals that we, we were saying, well, when is this going to happen, they weren't quite sure. So that's alarming. But I just want to ask, we have a couple of questions, I just, and any of you can answer if you'd like. Ah, here's one. The US Department of Defense has implemented a cyber security certificate requirement for potential vendors to get a contract.

Um, do you believe that New York City should do, take a similar approach to their contractors?

DANIEL GOLANSY: To their contract, to the contractors specifically?

CHAIRPERSON HOLDEN: Yeah. So you have to have a certificate...

DANIEL GOLANSY: Yeah, so...

CHAIRPERSON HOLDEN: ...a cyber security certificate, whatever that is.

DANIEL GOLANSY: Depending on, depending on the circumstances.

CHAIRPERSON HOLDEN: Right.

DANIEL GOLANSY: Right, I mean, if it's a contractor providing, you know, asphalt or concrete then perhaps it's not appropriate, right? If it's a contractor providing...

CHAIRPERSON HOLDEN: Well, they have, they have data, though. They have, you know, so...

DANIEL GOLANSY: Sure, yes, of course. Um, or, or perhaps the types of, there should be multiple types of certificates, of different gradations, those that would be appropriate for companies who provide equipment for this room, audiovisual equipment, right, ah, and other companies

that provide equipment that is integral to the technological infrastructure of the city versus those that are more traditional not cyber-related businesses. Sure, it would make sense, yes. I think that that would be a very, it's a start to solving a very large problem.

CHAIRPERSON HOLDEN: All right, good.

STEVEN BELLAVIN: I'm not always fond of some of these certificate programs because one size doesn't fit all when it comes cyber security. Every business is different, what they do with the data, even if they're in the same business they're operating very differential and the checklists tend to be either so broad as to be almost meaningless, or so specific that they end up being giant exercises in paperwork that don't actually provide a measurable improvement in the company cyber security stance. It's not a bad thought. I would actually look more towards a liability regimen and say OK, if you get hacked it impacts your business with us, or your customers, then you are liable and that would let the market respond in appropriate fashions. I think that would be more valuable than a certificate.

DEREK SHANAHAN: That's a very good point. And, tangentially, in the private world there is an ever-growing phenomenon of having this vendor risk management concept, where you have to have X amount of cyber liability to even do business with some of the biggest companies, like the Amazons of the world. So in effect you see it at the national level. In the public sector you see it and in kind of the private sector, very, very growing. Um, we get new requests every day because companies have to X amount of million dollars of cyber liability and so that almost skips around the, the nature of having the variety of types of businesses, because if you have a million dollars, two million dollars of cyber liability coverage and intentionally broad as you write a policy then that should capture most of the risk that you're doing, you know, that you have by doing business with a, a number of different vendors, so.

CHAIRPERSON HOLDEN: Um, do you want to testify, would you like?

UNIDENTIFIED: No, it's all good [inaudible].

CHAIRPERSON HOLDEN: OK, all right. All right. Just another question. Um, I'm gonna ask this, ah, recently the United Kingdom introduced a bill requiring IOT manufacturers to explicitly state the minimum length of time of which devices will receive security updates at the point of sale and provide a unique password. Should New York City follow the same approach, in your opinions?

STEVEN BELLAVIN: Yes. Ah, the, the really bad problem with IOT is that devices last a lot longer than typical support lifetime. It's an economic question of who is going to pay for continued support, and if no one is going to pay it becomes a, you know, a serious risk to everybody else on the internet because hacked IOT devices already have been involved in serious, large-scale, nationwide outages. So people need to understand, ah, the limits and, again, possibly liability. If you are operating something, a device that's involved in an attack maybe you should be liable, but you need to understand the support lifetime is going to be. It's fundamentally an economic problem. Who is going to pay for either a device that lasts less time than

the rest of its components would, or for the continued software [inaudible].

CHAIRPERSON HOLDEN: So what would you say is a reasonable amount of time?

STEVEN BELLAVIN: It's going to depend on the device. Cars last 15, 20 years. I want to make sure the, you know, a modern car has 60 or 70 computers in it and I want to make sure that I can keep driving that car for 15 years. Ah, you know, a internet-connected coffee pot I don't mind replacing after three to five.

CHAIRPERSON HOLDEN: OK, yeah, OK.

STEVEN BELLAVIN: But there is, you've got to work the economic...

CHAIRPERSON HOLDEN: Yeah, there's no, there's no one-size-fits-all, yeah.

STEVEN BELLAVIN: There's no one-size-fits-all.

CHAIRPERSON HOLDEN: All right.

STEVEN BELLAVIN: A disclosure requirement would be a really good first step and we should look into liability for operating device that's not supported.

CHAIRPERSON HOLDEN: Great. Anybody else?

DANIEL GOLANSY: Um, I actually have to respectfully disagree and, ah, say that I, I do not think that the city should institute that sort of policy. Um, and while I, I agree that there are significant issues with, ah, IOT devices, that's, that's for sure, ah, my concern is that we have an increasingly balkanized regulatory environment for all of these manufacturers, and we are deceiving ourselves into thinking that we can legislate our way out of this problem, ah, when this is the type of fast-moving problem that does not lend itself to those sorts of solutions. So while I see the, the intent there is good, I understand, and I, I would love the idea of having a, an out-of-the box IOT device with a unique password, right, that's terrific. I just think from a larger-scale perspective we need to be thinking about the issue of cyber security for individuals and for small businesses and for large businesses differently from the way we have thought about other security and criminal issues in the past.

CHAIRPERSON HOLDEN: So you, so you think it would, um, give somebody, the customers, a false sense of security, number one, if you had these, these passwords, let's say, built in, but also push up the price? Would that, of the, of the item?

DEREK SHANAHAN: No, that's, so pushing up the price I'll put aside. I think that, and I don't know the specifics on it. My suspicion is that any increase in price would be, you know, marginal at best. It, it is the larger-scale mentality that we as a city and even larger than that, as a country, need to have about cyber security and this idea that we can legislate our way out of the problem, when I just don't think that that's a realistic approach. Ah, we have a variety of regulatory regimens and I think that all of the intent there is terrific. Obviously, people are trying very hard to do the right thing. What I'm saying is that because of the nature of the problem it does not lend itself, it's a fast-moving problem, as opposed to traditional crime, which is slow moving, right?

CHAIRPERSON HOLDEN: Right.

DEREK SHANAHAN: The analogy about the robbing of the house. In the context of a fast-moving

problem the, the law is, the law almost never keeps up with technology.

CHAIRPERSON HOLDEN: Right.

DEREK SHANAHAN: And that, therein lies the problem.

CHAIRPERSON HOLDEN: And of course many people will say government is the problem also. It's, you know, like you said, there's too many regulatory, ah, things put on businesses anyway. Um, and I, I, what I've heard from the panel is it's really more of a simple problem and just, you know, an ounce of prevention, um, and, and back up your, you know, your devices and, ah, put protection that, you know, something very simple, like you mentioned, um, and be prepared. Um, which is, surprisingly small businesses are, are not. But, um, I'm just concerned with government not doing the proper outreach and, or maybe going down the wrong road, like some of you mentioned. Um, so we can't legislate our, our way out of this, right? We can't require, if somebody has a data breach, you're, you're all, I mean, I don't know if you're all saying this, but I know you were saying it, that we shouldn’t require them to call 911, or the police are

not going to do anything on this one. Ah, they never catch these guys. Um, but should it be reported at all?

DEREK SHANAHAN: So let me be clear. It's not that I said that they shouldn't, the reason I said that they should not call 911 is that I don't view that as an effective mechanism of addressing the problem.

CHAIRPERSON HOLDEN: No, I don't think anybody does.

DEREK SHANAHAN: Right.

CHAIRPERSON HOLDEN: But that's what they said that you should do.

DEREK SHANAHAN: Right, right. And I think that that's, and again, I think everyone has great intentions. I think that that's just not the right approach. Um...

CHAIRPERSON HOLDEN: But, but, just to follow up, should we require that they report it, doesn't have to be to the police, but should we know how many cyber attacks are happening?

DEREK SHANAHAN: Data is...

CHAIRPERSON HOLDEN: Like should we keep that data?

DEREK SHANAHAN: Data is of crucial importance.

CHAIRPERSON HOLDEN: Right.

DEREK SHANAHAN: The, the it there, I think depends significantly, right. I don't want to say every business should report it when the it can vary tremendously from...

CHAIRPERSON HOLDEN: Sure, sure.

DEREK SHANAHAN: ...situation to situation. But what I, from a broader perspective, if you look at a variety of problems that we have in our city and our society in a larger sense, ah, we have private groups that may have some attachment to government, but they are not in government directly, that can move faster, right? Um, um, I'm picking one out of, out of, so the AARP, right, the programs of, of retirees, right, they're not necessarily addressed by government directly always, sometimes they are, sometimes they're not. But there's an advocacy group. What I'm advocating for is that we have a group and that that group has the capacity, because they are separate from government, to move very quickly and to work integrally with government when appropriate.

CHAIRPERSON HOLDEN: So do you have something, a recommendation on how we get that group together, do you have, um, some, some, a paper that you can give us about this, this group?

DEREK SHANAHAN: Like an outline?

CHAIRPERSON HOLDEN: Yeah, an outline?

DEREK SHANAHAN: I don't have a paper off the top of my head, but I can prepare one for you if you like.

CHAIRPERSON HOLDEN: Yeah, if you, if you, yes, because I'd like to hear that.

DEREK SHANAHAN: If you, if you wish I'd be happy...

CHAIRPERSON HOLDEN: I will, I will...

DEREK SHANAHAN: ...to prepare an outline for you...

CHAIRPERSON HOLDEN: Right.

DEREK SHANAHAN: ...an outline for you and describe how best it can be assembled, or, in my view...

CHAIRPERSON GJONAJ: A vision.

DEREK SHANAHAN: Yes, in my vision how best it can be assembled.

CHAIRPERSON HOLDEN: Yeah.

DEREK SHANAHAN: And I'd be glad to provide that to, to the council, of course.

CHAIRPERSON HOLDEN: Yeah, 'cause I'd rather not have government do it, all of this, because we don't, I don't think they're as effective sometimes as a group of professionals who deal with this and who, you know, work at start-ups and, and or some kind of group that would meet and come up with ideas for government.

DEREK SHANAHAN: All of you want to do good.

CHAIRPERSON HOLDEN: Right.

DEREK SHANAHAN: There's no doubt about that.

CHAIRPERSON HOLDEN: Yes.

DEREK SHANAHAN: And you work very hard to do that good, right?

CHAIRPERSON HOLDEN: Right.

DEREK SHANAHAN: And what I'm saying is, exactly. It, it is so beyond the pay grade of government that it's time for government to call in the special forces.

CHAIRPERSON HOLDEN: OK, great. I love that idea.

STEVEN BELLAVIN: So, ah, as I've said, I've been working at the national level on reporting, ah, you know, one of the reasons that commercial air travel is so safe is that every crash is investigated by the NTSB. From there, there are recommendations to manufacturers, airlines, pilots, and so on what to do differently. And that's why commercial aviation is so safe. A second component is a voluntary near-miss reporting system that's run by Miter on behalf of NASA, where you basically report anonymously something that almost results in disaster, and again, this has resulted in tremendous improvement in air safety, and I've published an essay on a, what I call the major cyber incident investigation board and a longer law review article on a voluntary reporting system. I think that any time there's a data breach that's reportable under the SHIELD Act, I think there should be reporting to a state agency, not just of the facts of the breach, but enough details to let professionals understand what went wrong. I think a voluntary system at the state level, there is a role for legislation, regulatory and legal forbearance for voluntary reporting of near-misses. You don't want to expose yourself to liability, that's one of things

why this is a law review article, ah, published, I think, about two years by, by disclosing something that might, again, this has worked very for aviation and a number of other fields, and we need to do it. The industry needs data on what exactly went wrong, and it's not generally as simple as somebody phised my password. There tends to be a whole chain of mistakes that led to the breach. The industry needs data. Researchers need data. The private sector needs data on how to improve its products and how to improve its response. And the only way we're going to get this is with reporting. Right now details are very hard to come by and we need to do something about that. We're not going to improve without data.

CHAIRPERSON HOLDEN: Great, great point. Thank you.

DANIEL GOLANSY: Yeah, I categorically agree with the other panelists that there should be some sort of required reporting. I mean, needless to say, ah, and I am biased, but there are a couple of agencies that have half in, half out type of a footing on cyber security at the national level. Surprisingly, the FDC has by technicality been the number one, um, if you will, ah, crime force on

national cyber crime. Just because how Congress is set up. And then also you have things like the Internet Crime Control Center, which is a reporting body that may or may not get the right data. You have insurance agencies that with claims information can come up with claims information can come up with some sort of speculation. But you're going to get competing numbers across the board. And so if you start not at the national level but at the city level, the City of New York being a perfect example of this with the SHIELD Act, I think that could be a, a terrific foundation for the rest of the large cities and then past that, the national level to adopt.

STEVEN BELLAVIN: I was, ah, spent a year as chief technologist of the Federal Trade Commission. I know intimately what, ah, it can and cannot do, and one thing it does not do typically is published detailed information on what went wrong. It's, almost all of its settlements involve consent decrees where there's some detail provided, but often not enough and they're only dealing with the, with the very biggest cases or the most egregious cases. As you say, they're the de facto regulator and only

for certain situations, not for others, because of their authority under the Federal Trade Commission Act. They do need more authority from Congress. I don't know that they're the best body to, ah, handle the more detailed kind of data gathering that I'm talking about. But, yeah, I point my students at some of their, ah, investigations all the time.

CHAIRPERSON HOLDEN: Oh, great. Do you have any questions?

CHAIRPERSON GJONAJ: I want to thank you for, ah, being here and your testimony on this, what is deemed to be a real threat, and I don't thing government is taking the initiative and priority that it should by investing, um, into cyber security. Ah, it is threatening society. It is a threat to the, um, economic development. It is a threat to, ah, and we forget that we dub small businesses as businesses. They're New Yorkers. They're no different than, um, they should be protected, ah, and valued, just like our citizens are. Without them this would be a different city. And I agree with you, gentlemen, that New York tends to lead the way and, um, or what New York does other states follow. Um, this is going to be, there are some very difficult challenges and a

heavy lift, um, and I don't know if we can get right in the beginning, but all things need to start somewhere, ah, and then we can make adjustments. So thank you for your valued expertise and being a part of testimony, as we now take on the burden of determining now that we know what do we do next. And we'll continue that dialogue. Thank you.

UNIDENTIFIED: Thank you.

UNIDENTIFIED: Thank you.

CHAIRPERSON HOLDEN: OK, thank you all for your great testimony. I, I want, um, obviously, I'll give you my card and I think we should, ah, exchange numbers to, ah, to talk further about this, because I think you, you provided great, great testimony and another look at what we should be doing in cyber security. So thank you all again for your public service, and thanks for waiting for so, so long. Thank you. All right. [gavel]

C E R T I F I C A T E

World Wide Dictation certifies that the foregoing transcript is a true and accurate record of the proceedings. We further certify that there is no relation to any of the parties to this action by blood or marriage, and that there is interest in the outcome of this matter.

Date March 26, 2020