Committee Meeting

of

SENATE LAW AND PUBLIC SAFETY COMMITTEE

"The Committee will hear testimony from invited guests on cybersecurity issues affecting New Jersey, including, but not limited to, the implementation of P.L.2023, c.19, which requires certain cybersecurity incidents to be reported to the New Jersey Office of Homeland Security and Preparedness. Testimony will also be taken on the obligation of private entities to report these incidents"

LOCATION: Committee Room 10
State House Annex
Trenton, New Jersey

DATE: December 16, 2024
10:00 a.m.

MEMBERS OF COMMITTEE PRESENT:

Senator Linda R. Greenstein, Chair
Senator Paul D. Moriarty, Vice Chair
Senator Angela V. McKnight
Senator Owen Henry

ALSO PRESENT:

Amanda D. Holland
Thomas M. Kelly
Office of Legislative Services
Committee Aides

Tom Little
Senate Majority
Committee Aide

Gregory Harris
Senate Republican
Committee Aide

Meeting Recorded and Transcribed by
The Office of Legislative Services, Public Information Office,
Hearing Unit, State House Annex, PO 068, Trenton, New Jersey

Amanda D. Holland
Thomas Kelly

Office of Legislative Services
Committee Aides
609-847-3870

NEW JERSEY STATE LEGISLATURE

SENATE LAW AND PUBLIC SAFETY COMMITTEE

STATE HOUSE ANNEX • P.O. BOX 068 • TRENTON, NJ 08625-0068
www.njleg.state.nj.us

COMMITTEE NOTICE

TO: MEMBERS OF THE SENATE LAW AND PUBLIC SAFETY COMMITTEE

FROM: SENATOR LINDA R. GREENSTEIN, CHAIRWOMAN

SUBJECT: **COMMITTEE MEETING - DECEMBER 16, 2024**

The public may address comments and questions to Amanda D. Holland, Thomas M. Kelly, Committee Aides, or make bill status and scheduling inquiries to Michelle L. McArthur, Secretary, at (609)847-3870 or e-mail: OLSAideSLP@njleg.org. Written and electronic comments, questions and testimony submitted to the committee by the public, as well as recordings and transcripts, if any, of oral testimony, are government records and will be available to the public upon request.

The Senate Law and Public Safety Committee will meet on Monday, December 16, 2024 at 10:00 AM in Committee Room 10, 3rd Floor, State House Annex, Trenton, New Jersey.

The committee will hear testimony from invited guests on cybersecurity issues affecting New Jersey, including, but not limited to, the implementation of P.L.2023, c.19, which requires certain cybersecurity incidents to be reported to the New Jersey Office of Homeland Security and Preparedness. Testimony also will be taken on the obligation of private entities to report these incidents.

The following bill(s) will be considered:

S3944 Sarlo/Gopal	Provides that certain non-profit corporation alcoholic beverage theater licensees include disregarded entities of such corporations.

Issued 12/10/24

For reasonable accommodation of a disability call the telephone number above or for persons with hearing loss dial 711 for NJ Relay. The provision of assistive listening devices requires 24 hours' notice. CART or sign language interpretation requires 5 days' notice.

For changes in schedule due to snow or other emergencies, see website http://www.njleg.state.nj.us or call 800-792-8630 (toll-free in NJ) or 609-847-3905.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

TABLE OF CONTENTS (continued)
APPENDIX (continued)

SENATOR LINDA R. GREENSTEIN (Chair): I don't think I even have to call you to order, you're all so-- Oh, this is so nice. Everybody is just waiting.

I'm sorry about that. Don't take Route 1 in either direction; it's a parking lot.

So, can I ask for attendance?

MR. KELLY: Senator Henry.

SENATOR HENRY: Here.

MR. KELLY: Senator McKnight.

SENATOR McKNIGHT: Here.

MR. KELLY: Senator Moriarty.

SENATOR PAUL D. MORIARTY (Vice Chair): Here.

MR. KELLY: Chairwoman Greenstein.

SENATOR GREENSTEIN: Here.

MR. KELLY: You have a quorum.

SENATOR GREENSTEIN: OK, thank you; thank you.

We are going to start with the bill that we have. We only have one bill today: Senator Sarlo's bill.

OK, this is Bill Number 3944, Sarlo and Gopal. Provides that certain nonprofit corporation alcoholic beverage theater licensees include disregarded entities of such corporations.

Are there any amendments?

MR. KELLY: No amendments.

SENATOR GREENSTEIN: OK.

Do we have anybody to testify?

MR. KELLY: No.

SENATOR GREENSTEIN: Nobody to testify on the bill.

MR. KELLY: Oh--

SENATOR GREENSTEIN: I'm sorry--

UNIDENTIFIED SPEAKER: Madam Chair, (indiscernible)

SENATOR GREENSTEIN: Do you have it?

MR. KELLY: I don't have the slip--

SENATOR GREENSTEIN: OK, have them come up.

And, would you make sure you do a slip before you go, so we have that for the record?

Thank you.

D O R E E N S A Y E G H: Good morning, Chairwoman--

SENATOR GREENSTEIN: Good morning.

MS. SAYEGH: --Committee members, Senators.

Thank you so much for giving me the opportunity to speak this morning.

My name is Doreen Sayegh. I am the owner and operator of the Cranford Movie Theater in downtown Cranford.

I grew up in the movie theater business; my father owned many theaters across New Jersey. He was the largest independent movie theater owner in the 1990s. So, I have a passion and a love for this industry. It is a place where magic happens, and community comes together.

I know the bill is on behalf of nonprofit theaters; we are a for-profit theater. There's not many of us left on the independent side. So, this bill would be very important and crucial to our vitality and our future in the industry. Before COVID, there were more than 100 theaters -- movie theaters -- in New Jersey. Over 28 have closed after the pandemic. We were

struggling before the pandemic, because we're competing with streaming devices, peoples' changing habits. There's just so much out there that we're up against. And, yet, we've been a very resilient industry. We've been creative; we've partnered with our community; we've partnered with charities; we've done so much.

I took over the Cranford Theater in 2019 after the tenant abruptly abandoned the theater. But, it's such a beautiful town, and so vibrant, and full of families and young children. We renovated the theater in October 2019, opened in November 2019, and were shut down by the pandemic in March of 2020. In that time, we started selling candy and concessions to pay our bills and keep up with property taxes. A few months later, we got wind of the drive-in making a comeback, and I've always wanted to be in that business. I've never been to a drive-in. So, we put a model together, and within two months, erected a drive-in theater in a parking lot in the municipality. This drive-in sold out for six months, six nights a week. People came from all over New Jersey and New York and Pennsylvania to support and to enjoy a night out, because there really was nothing else to do during that time.

Because ticket sales were off to a strong start and we didn't have to focus our efforts on that, we then turned our efforts into what can we do for the community, and how can we find ways for them to help? We found our way, which was providing entertainment in a tough time. So, in that time, we raised money for the Children's Specialized Hospital; we did fundraisers for underprivileged schools that didn't have school supplies, cleaning supplies. We did holiday wrapping supplies; we did a food drive; and we made it fun. We kicked it off with a movie and costumes and

inflatable dinosaurs in the parking lot, just to create experiences for people to have a good time and to escape the reality of what was going on around us.

Movie theaters create an immersive experience; we create lasting memories. And, I for one, who grew up in movie theaters, can tell you I'm full of memories. So, I have so much to say and so little time, but we, too, provide the same experience as nonprofit theaters. We go above and beyond. We don't have the same opportunities; we're not eligible for grants and donations and things like that. When we get in trouble and our operating account sinks, we're dipping into our personal funds. We want to keep our theaters alive. We know the magic these buildings -- they are anchors in their towns, and, I'm sure the town of Cranford can vouch for me. The theater has been an anchor; it has brought so much vitality and so much business to all the surrounding businesses.

A liquor license would be so helpful for *our* theaters, too. Not just mine -- all movie theaters. And, I can tell you just a few examples. It would attract new events and performers -- comedy shows, more upscale events and more upscale audience. A glass of wine with a Metropolitan Opera or a ballet. And, it would also create a revenue stream to help support the theater's sustainability.

It's no secret that theaters are closing left and right. I could tell you there's probably going to be a few more next year in New Jersey that are going to close, because they're struggling. It's a hard business to be in. But, I love it, and I believe in it, we do-- All of us theater owners believe in what we're doing. I could tell you, this weekend we had a pajama party series at the theater. We do it every weekend leading up to Christmas. It's based off my childhood memory of growing up in my dad's theaters where, in the '80s

-- not to date myself -- but Santa would come on the fire truck and he would hang out in the lobby and you got to take pictures and he gave you a little knickknack. So, we've done it. We started with two weekend shows, and it's now expanded to five. People come from all over New Jersey; they come from New York and Pennsylvania to join us. They get to watch a movie; they come in their PJs; and we work with the Fire Department so that we tie in our community members to partner with us. And, they bring Santa and Mrs. Claus and deliver them to the theater, and everybody goes wild.

So, we bring-- We bring so much effort; we do so much for the community. And this can really be really beneficial and really help us sustain and last, and just introduce new events and opportunities to our theaters.

Thank you.

SENATOR GREENSTEIN: OK--

MS. SAYEGH: There's so much more, but I know -- we're limited.

SENATOR GREENSTEIN: Thank you very much.

MS. SAYEGH: Thank you.

SENATOR GREENSTEIN: And, very good -- it shows your enthusiasm--

MS. SAYEGH: I love it, it's magic, it really is.

SENATOR GREENSTEIN: Any questions or comments?

SENATOR McKNIGHT: I have a question.

SENATOR GREENSTEIN: Sure.

SENATOR McKNIGHT: Thank you so much for your testimony.

Have you reached out to the senator, Senator Sarlo, in reference to this update?

MS. SAYEGH: No, I have not. But, that is actually our next step.

So, I'm actually very eager and very excited.

SENATOR McKNIGHT: Yes--

MS. SAYEGH: There's really so much. I mean, I could tell you, we've had marriage proposals, engagements -- you name it, we've done it.

SENATOR McKNIGHT: So, please do that.

MS. SAYEGH: Thank you.

SENATOR McKNIGHT: Sooner than later--

MS. SAYEGH: Yes--

SENATOR McKNIGHT: --and thank you so much for your testimony.

MS. SAYEGH: Oh, no, I appreciate it.

I welcome you to come to Cranford and just-- We just recently did an event with Armand Assante, who played Gotti. He came into the theater; we raised money for the Garden State Film Festival. So, there's really-- There's so much that can be done.

So, thank you so much. I appreciate it.

SENATOR MORIARTY: I just wanted to comment.

I love your mission--

MS. SAYEGH: Thank you.

SENATOR MORIARTY: I love-- I wish I could be there on the 21st for *Elf*.

MS. SAYEGH: Thank you--

SENATOR MORIARTY: It's $9 a ticket if anyone is listening, which is a bargain.

I love the mission. Drive-in movie theaters were founded in New Jersey--

MS. SAYEGH: Yes--

SENATOR MORIARTY: Camden, New Jersey--

MS. SAYEGH: Camden, New Jersey -- actually, so was filmmaking, Fort Lee--

SENATOR MORIARTY: Yes, in Edison.

So, we have a long history with the movies, and I love that you are keeping the mission going.

MS. SAYEGH: And, we do. And, we're very big supporters of the Film Commission, and the tax incentive, and all the filmmaking that's taking place in our state.

We actually -- I forgot to tell you this -- we actually have-- We host high school students who are in film classes, and we bring the film -- somebody from the Film Commission to speak to them about filmmaking, and one day their movies are going to be on our screen.

So, we're big supporters of film festivals and independent filmmakers. There's always something for everyone.

SENATOR MORIARTY: Anything we can do to help keep the mission going--

MS. SAYEGH: We appreciate it--

SENATOR MORIARTY: --because it's important to have these independent movie theaters--

MS. SAYEGH: I would hate to see them close.

SENATOR MORIARTY: So, please reach out--

MS. SAYEGH: Thank you--

SENATOR MORIARTY: --to the Senate President so that we can perhaps amend this bill to help you as well.

MS. SAYEGH: Thank you.

SENATOR MORIARTY: Thanks for coming here today.

MS. SAYEGH: We really appreciate-- Thank you so much. I'm sorry.

SENATOR GREENSTEIN: Thank you very much.

MS. SAYEGH: Thank you.

SENATOR GREENSTEIN: Can I get a motion.

SENATOR HENRY: Move it.

SENATOR GREENSTEIN: Thank you.

SENATOR MORIARTY: Second.

SENATOR GREENSTEIN: Motion and second.

MS. SAYEGH: Thank you so much.

SENATOR GREENSTEIN: Thank you.

MR. KELLY: On the motion to release Senate Bill 3944. Senator Henry.

SENATOR HENRY: Yes.

MR. KELLY: Senator McKnight.

SENATOR McKNIGHT: Yes.

MR. KELLY: Senator Moriarty.

SENATOR MORIARTY: Yes.

MR. KELLY: Chairwoman Greenstein.

SENATOR GREENSTEIN: Yes.

MR. KELLY: The bill is released.

SENATOR GREENSTEIN: Thank you.

MS. SAYEGH: Happy holidays.

SENATOR GREENSTEIN: Same to you.

MS. SAYEGH: Thank you so much.

SENATOR GREENSTEIN: OK, and now -- now we're going to start our hearing on cybersecurity.

Now, we're going to have a number of speakers today, but this may be the first of several that we might have. And, I thought the goal here is to talk about the issues and then decide what legislation might be needed. We've done a couple of bills, but we may very well need more.

And, so, I want to begin by thanking everyone here this morning, and extend a special thank you to the invited speakers who are here today to share their expertise and knowledge on cybersecurity, an issue that grows more important with each passing year.

Every facet of our lives has become increasingly digitalized, and this trend does not just extend to our private lives and entertainment. Government, healthcare, and all sorts of private businesses are now intertwined with technology. And, while that has brought immense benefits, it's also brought new threats.

Today's hearing is meant to gather firsthand expert testimony from those who are most familiar with the topic to hear about how current laws surrounding cybersecurity has been implemented, and to find out more about what can be done to proactively address these new challenges.

So, thank you very much, and we will begin. We're going to start with the world of government, and we'll start by hearing Michael Geraghty,

Director of the New Jersey Cybersecurity and Communications Integration Cell -- or NJCCIC -- and the State's Chief Information Security Officer.

And, I do remember that you testified a couple of years ago in front of this Committee, and I am interested in hearing what's developed since then, and how things are going. I know we hear of many instances of cybersecurity problems.

So, thank you for coming.

M I C H A E L G E R A G H T Y: And, thank you for having me.

So, Chairwoman Greenstein, Vice Chairman Moriarty, and distinguished members of the Committee, thank you for the opportunity to testify today about the critical importance of cybersecurity incident reporting, and the evolving threat landscape facing our state.

The mission of NJCCIC -- the New Jersey Cybersecurity Communications Integration Cell -- is to lead and coordinate New Jersey cybersecurity efforts while building resiliency to cyberthreats throughout the state. As part of that mission, I, as the Chief Information Security Officer, have primary responsibility for establishing and managing a cybersecurity program that ensures the confidentiality, integrity, and availability of New Jersey CCIC Executive Branch systems, resources, and services.

Additionally, the NJCCIC provides cybersecurity threat mitigation and incident response services to all New Jersey public- and private-sector organizations and the general public.

New Jersey's public-sector and private-sector institutions, as well as its residents, face a consistent and credible threat of cyberattacks from multiple types of threat actors, with varying capabilities and motivations. Nation-state actors, such as China, Russia, Iran, and North Korea have

targeted American companies and infrastructure for espionage and potential disruption of critical systems. Transnational cybercrime syndicates, such as LockBit, Clop, and BlackCat/ALPHV continue to conduct financially motivated ransomware attacks on all manner of organizations, including hospitals; local governments; law enforcement agencies; large and small businesses; and educational institutions. The threat landscape we face today is more complex and dangerous than ever before.

In 2020, the NJCCIC detected and blocked approximately 10 million attacks targeting New Jersey's Executive Branch network systems applications and users monthly. Today, the NJCCIC detects and blocks more than that many attacks daily. Several factors contribute to this almost 30-fold increase, including -- but not limited to -- the state's expanding use of technology to support all aspects of its daily business functions and critical services. The resulting increase of its attack surface? The increasingly complex global environment whereby networks, systems, applications, and users can be subject to attacks from anywhere in the world at any time of day or night and the NJCCIC's enhanced monitoring capabilities.

Beyond the Executive Branch, as of December 11 -- when I wrote this testimony -- the NJCCIC has documented 4,989 ransomware cases worldwide this year. That's an 18% increase over 2023; with 66 New Jersey organizations directly impacted, a 10% increase over 2023. These attacks are operationally debilitating and financially costly to the New Jersey healthcare providers; municipal water systems; law enforcement organizations; educational institutions; and other critical infrastructure and key resources that are impacted. These attacks also resulted in the compromise of sensitive personal information of thousands of New Jersey residents.

We face sophisticated threats from nation-state actors who see New Jersey's critical infrastructure, intellectual property, and government systems as attractive targets. The Volt Typhoon campaign -- attributed to China's People's Liberation Army, the PLA -- has already compromised nearly two dozen critical infrastructure organizations across the United States. More recently, Salt Typhoon -- which is also attributed to the PLA -- has been implicated in compromising eight major telecommunications providers in the United States. Iranian-backed groups, like CyberAv3ngers, have specifically targeted water and wastewater utilities nationwide. Russia's intelligence agencies -- particularly the foreign intelligence service, the SVR, and the main intelligence director GRU -- have also carried out numerous attacks against United States public- and private-sector organizations, including attacks on our elections infrastructure and key information technology suppliers.

A Russian hacktivist group -- the Cyber Army of Russia Reborn, which is linked to the GRU -- has carried out attacks and compromised the networks of energy and water sector organizations, including the operational technology infrastructure of at least three New Jersey water systems. The threats we face are persistent and evolving. They have the potential to adversely impact public health; the welfare and safety of our residents; the economy and public interest in the state; and national security.

As for cybersecurity incident reporting -- the bill that I previously testified on-- In 2024, the NJCCIC has thus far received 493 cybersecurity incident reports through its incident-reporting portal. A hundred and forty-six of these incidents have been reported by public agencies in accordance with P.L.2023, c.19. In 2023, when the law was enacted, the NJCCIC received 141 cyber incidents from public agencies. And, in 2022 -- the year

prior to the bill -- the NJCCIC received 96 reports from public agencies. In addition to the reports made to the NJCCIC via its reporting portal, the NJCCIC also proactively notifies organizations whose information technology infrastructure has been compromised, or whose networks contain vulnerabilities that could be exploited by threat actors. The NJCCIC does this as the result of indicators of compromise it detects; information provided by trusted third parties; and other open and commercial sources of intelligence. In 2024, the NJCCIC has thus far notified 167 public-sector and 49 private-sector organizations that their information technology infrastructure has been compromised.

Timely and thorough reporting of cybersecurity incidents via NJCCIC is essential for the following four reasons:

1. Enhanced response and recovery. When incidents are reported to the NJCCIC, effective organizations gain access to specialized expertise, including threat analysis; remediation guidance; and coordination with law enforcement and other resources that can provide response and recovery assistance. In addition, the reporting entity can receive assistance in implementing controls to bolster their cybersecurity posture, to help ensure they do not experience a reoccurrence.

2. Improved threat intelligence. Each report helps the NJCCIC build a clearer picture of the threat landscape, allowing for the identification of emerging trends. For example, reports of phishing campaigns and ransomware attacks have informed the advisories and alerts the NJCCIC has published, that help other organizations prevent similar incidents.

3. Preventing cascading failures. Cyberattacks have ripple effects. Reporting incidents allows the NJCCIC to warn potentially impacted sectors and prevent wider disruptions.

And, then, 4. Strengthen public- and private-sector collaboration. Incident reporting fosters collaboration between public agencies, private businesses, and the Federal partners, creating a unified defense against cyberthreats. This collaboration is vital in addressing systemic risk.

As we look to the remainder of 2024 and beyond, we face new challenges from emergent technologies. The increasing pace of change and rapid technological advances in areas such as elastic cloud computing; artificial intelligence; autonomous systems; big data; and the internet of things enables modern society to address classes of applications that were inconceivable just a few years ago, while also creating an internet of everything -- comprised of physical and virtual objects; people; processes; and data. This digital transformation and our growing dependence on the confluence of technologies is expected to continue unabated for the foreseeable future, creating an expanding attack surface, and provides opportunities for nation-states, terrorist organizations, political activists, and criminals to maliciously target cyberinfrastructure and information for foreign policy; national interest; financial gain; fulfillment chaos and anarchy; social divisions; and for other nefarious motivations.

In conclusion, it is unrealistic to expect any one person or organization to defend against nation-state actors, or criminal syndicates, or hacktivists, cyberterrorists and other threat actor groups who can launch attacks from anywhere in the world at any time of day or night. Effectively

managing cyber risks requires a proactive and collaborative approach. Our collective security depends on sharing information about the threats and incidents quickly and accurately. Public- and private-sector organizations at the Federal, State and local levels, as well as businesses large and small, *must* collaborate by sharing threat intelligence, implementing robust cybersecurity standards, and fostering a culture of vigilance.

The NJCCIC incident reporting system has proven its value in our collective defense efforts, but we must continue to strengthen and expand these capabilities to protect our state's private- and public-sector organizations, critical infrastructure and key resources, and its residents.

Thank you for your attention to this crucial matter, and I welcome any questions.

SENATOR GREENSTEIN: Thank you so much; that was great.

There could be a hundred questions for you, because you're at the -- really, at the center of this.

It's inevitable that somebody will ask a question about drones. So, I'm going to be that person -- at least now -- but we don't want the hearing to go off in that direction, because maybe our next hearing will be about that. Most of us have no idea what's going on. But, I do have to say, in watching people on TV, I was really listening to them, and they were speaking in a very roundabout way. I was totally confused listening to elected officials and others.

I mean, is that something that your department gets involved in, and how are you involved with that? If you are.

MR. GERAGHTY: Sure.

So, the Office of Homeland Security Preparedness -- which is where I report into with the NJCCIC -- yes, does get involved with the drone activity that's happening now, as well as all those preparedness efforts; counter UAS systems and the like. So, we work with the State Police, our Federal partners in the Department of Homeland Security, the FBI, and others.

After the attacks of 9/11, the State created a Domestic Security Preparedness Task Force -- which is not just the Office of Homeland Security Preparedness, but all those cabinet members, whether it be the State Police, the National Guard -- all those others that are required to put together mitigations to prevent terrorist attacks or any electronic attack or a drone attack like we're talking today.

So, yes, we're involved. Unfortunately, I don't have all those answers that *everybody* wants, but I can tell you that we are working around the clock with our partners to resolve it.

SENATOR GREENSTEIN: One last question on this.

People on TV were saying that we have nothing to worry about, and they said that they've heard that. But, how do people know we have nothing to worry about?

MR. GERAGHTY: I don't know where they got their answers, or the information they provided.

SENATOR GREENSTEIN: Yes, that seems to be the case.

And, then, in terms-- Can you just briefly explain ransomware?

MR. GERAGHTY: Sure.

So, ransomware is malware, OK, like a virus that we used to know and love. Unfortunately, the way it's used is for extortion purposes. So, a

threat actor gains access to a victim's network, OK, implements ransomware -- that virus or malware -- exfiltrates or takes all the sensitive data out of the entity that's impacted, and then launches the ransomware that encrypts all the files on all the systems across the network -- thereby putting double pressure -- not just single pressure of ransomware, but the exfiltration that if you don't pay a ransom, what's going to happen is we're going to leak your sensitive information.

SENATOR GREENSTEIN: Legislatively speaking -- and, I think we talked about this the last time, too -- do you think -- can you think of things that we as the Legislature could be doing; legislation we might put forth that might help in the work that you're doing?

MR. GERAGHTY: I think anything and everything we can do together, whether it's legislation or the vigilance that I was talking about; the incident reporting. All of those things, we're doing it in public agencies today.

And, I know we've had these conversations regarding critical infrastructure in New Jersey. Every major hospital system in New Jersey has been victim of a ransomware attack. *Many* of those attacks have resulted in ambulances being diverted and surgeries being postponed. It's had impacts on patient care.

Same thing with water and other sectors of the critical infrastructure sectors, where these are not *just* extortion demands and information that's being leaked; these are actually public health and safety issues that are really impactful.

And, I go back-- We mentioned 9/11 a little while ago, and former Governor Kean was the Co-Chair of that. And, this stays on my bulletin board and it's been on my bulletin board since I took this job in

2016. On that September day, we were unprepared; we did not grasp the magnitude of a threat that had been growing for some considerable period of time. This was a failure of policing; a failure of management; a failure of capability; but, above all, a failure of imagination. And, I think we have to start thinking beyond just solving yesterday's problems.

But, as we increase our use of technology across *all* sectors, we have to imagine that those problems are going to occur at some point and be prepared. One, we should be mitigating them, but also responding to them.

SENATOR GREENSTEIN: Are a lot of them coming from other countries?

MR. GERAGHTY: Yes, a lot of them are coming from other countries. I don't have the breakdown, but I can tell you that during the election period -- the 10 days of the early voting, and then final election day -- Argentina was the Number 1 attacking country. And, it *doesn't* mean that the Argentinians hate New Jersey and were carrying out those attacks. It just means that infrastructure being used there was used to target New Jersey's election system.

So, when we say it's coming from other countries, we have to be careful. We can say it's coming from the infrastructure in other countries, but it doesn't mean the *people* in those countries are carrying out those attacks.

SENATOR GREENSTEIN: And, I get-- One of the reasons I asked that is I was thinking of punishing the people who are doing it. But, if many of them are hidden in other places, it may not be possible.

Do we-- How much do we punish them for what they've done?

MR. GERAGHTY: So, overseas, it's really difficult. So, ransomware groups, Eastern European ransomware groups -- Russia, Ukraine, other places like that -- they're not punished, and there's no extradition treaty, so the FBI does a great job in investigating; it takes them a long time. They may indict these individuals, and there may be a red notice that's filed with Interpol, so if they travel outside of Russia or around in places like that, they'll be arrested. But, that's not necessarily a deterrent.

SENATOR GREENSTEIN: Yes; that's unfortunate.

OK, questions?

Yes.

SENATOR MORIARTY: Thanks for being here.

What percentage of these cyber attacks has to do with trying to extract monetary gain, and what percentage might be foreign actors that just want to destabilize our government or some of our institutions? Do you know?

MR. GERAGHTY: I don't know their -- the number of them. But, I can tell you the majority of attacks, the main motivation is financial. Just like any other crime.

If you can monetize malware, you're going to do that. Business email compromised, phishing attacks -- all those different things. If there's an easy way to make money, people will do that. And, if you can do that remotely from overseas, that's even better.

As far as the nation-state actors, they may not be as prolific, but they are much better and more resourced. So, when they burrow into critical infrastructure systems, or can hack into what were previously thought to be very secure companies and the like, they have those capabilities -- whether it

be China, Russia, Iran, North Korea, and then others as well. And, they've been doing that for years, and years, and years for espionage. The Volt Typhoon, as I mentioned, is a campaign by China's PLA that is more to pre-position themselves within the critical infrastructure of the United States so in the event of a conflict, they can turn off electricity; they can disrupt communications; they can do those things.

So, while those attacks and the incursions are not necessarily destructive right now, it's what we call preparing the battlefield, if you will.

SENATOR MORIARTY: So, if the majority of these attacks are for financial gain, I imagine that because there is cryptocurrency, that is the way that they get paid.

MR. GERAGHTY: Yes, cryptocurrency laundering; all the different cryptocurrencies that are out there. That's-- They think it's untraceable; it takes some time to trace, but, yes, laundering cryptocurrency is the way they get paid.

SENATOR MORIARTY: So, if cryptocurrency were not available, many of these actors wouldn't bother because they would not be able to safely sit at a computer -- or wherever they are, in some foreign country -- and still be able to collect a ransom?

MR. GERAGHTY: I wouldn't go so far as saying it wouldn't be a problem. Threat actors are motivated, and they're going to find ingenious ways of getting paid. And, they were doing it before cryptocurrency--

SENATOR MORIARTY: Well, it's a lot harder if you have to actually--

MR. GERAGHTY: Yes--

SENATOR MORIARTY: --show up to get a bag of cash, as opposed to somebody just puts it into an anonymous account somewhere.

MR. GERAGHTY: Sure.

And, in the financial services arena, we have those "know your customer" laws. The same thing has to apply to the cryptocurrency arena. And, it's starting to get out there, but it's-- Not every cryptocurrency organization is following those rules.

SENATOR MORIARTY: So, I think this is a big problem, cryptocurrency, personally, because I think it's the currency of thieves and robbers and pirates and druggies and -- I see no use for it, although it's now, I think, $105,000 a bitcoin. I don't know what all these smaller things are -- dogecoins, and whatever they are.

But, do you see a role for government to do something about further regulating an industry that's pretty much completely unregulated?

MR. GERAGHTY: Absolutely. I think the financial services industry, the regulations that apply to all those in that industry, should also apply to cryptocurrency.

SENATOR MORIARTY: Do you see that happening in Washington?

MR. GERAGHTY: I see some movement towards that, and even though we can control some of that or (indiscernible), cryptocurrency companies overseas may not follow those same rules. And, so, they're going to be used; they'll find a way to use those companies instead.

SENATOR MORIARTY: Switching gears, if we were to send -- if you were to send a phishing email to every state employee and every municipal employee that has an email account, what percentage of people do

you think would open that phishing email and then do something that is dangerous, such as click on a link; follow through on something? And, should we be testing people more frequently? Because if people-- We have thousands and thousands of people who have email accounts in the State. If they're doing dangerous stuff by opening and then clicking on things, it exposes all of our systems -- whether it's Treasury or Department of Health, whatever.

What percentage of people today -- still -- would open up a phishing email and do something that was not advisable?

MR. GERAGHTY: So, in the Executive Branch, I can give you numbers, because we do this and we've been doing it for the eight years that I've been the CISO.

First time doing it was about 30% of Executive Branch employees opened the email, clicked on the link, or downloaded the attachment. Today, it's about 10%, OK, which is a lot less. I can't talk about what it is in the public sector, but I imagine it's similar.

That being said, as a--

SENATOR MORIARTY: And, that's in the Executive Branch.

MR. GERAGHTY: The Executive Branch. That's all I have direct authority to do those--

SENATOR MORIARTY: Would you expect that to be the same, less, or more in other departments?

MR. GERAGHTY: I would expect it to be the same.

SENATOR MORIARTY: OK.

So, a third of the time when you start -- and, then you do some education, I guess?

MR. GERAGHTY: Sure; yes.

SENATOR MORIARTY: Is that an area that we should be doing something in terms of legislation requiring training; requiring these phishing expeditions to be sent out weekly, or monthly? Penalties for not adhering?

I mean, this is really putting our systems at risk.

MR. GERAGHTY: So -- yes. Training, absolutely.

As to the threats, the policies the organization has, the laws that are in place -- all those different things -- privacy. As far as phishing email tests -- and, I can tell you this -- law enforcement has to open emails, OK, because it may have a subject line that there's a crime. Human Resources -- if you send them something that says, "I've been sexually harassed," they're going to open those. We, in State Government and government all over, *have* to open those as public servants.

I think what we as CISOs -- the Information Technology and cybersecurity folks -- have to do is build systems that don't depend on nobody making a mistake by clicking on a link. I think that's a better use of our time, rather than trying to trick people into opening emails, or not opening emails.

SENATOR MORIARTY: Is it possible to create something like that?

MR. GERAGHTY: Yes, and that's why--

SENATOR MORIARTY: Why has it not been done?

MR. GERAGHTY: That's my job, to make sure, because we do get people who do click on phishing emails that are coming in, not just to test. What do we get -- three million emails sent into State Government workers on a daily basis, and many of them are being blocked because they contain malware or phishing content. But, there's stuff that gets through;

nothing is 100% perfect. And, so, we're going to have people clicking on those.

And, so, what we focus on is resilience; being able to detect that and then recover promptly, rather than saying something is going to be 100% secure. There's nothing like that.

SENATOR MORIARTY: Thank you very much for being here.

SENATOR HENRY: Just a follow up on what you said and where we should be focused.

Human error, technology -- where do you think, legislatively, we should be focused on making improvements? Human error -- we have a tough time telling people not -- as you said. Where do our efforts need to be focused? In your opinion.

MR. GERAGHTY: So, I think it has to be a holistic approach to cybersecurity. And, when I say that--

SENATOR HENRY: A successful attack, I'm sure you go back and found how they got into that system?

MR. GERAGHTY: Yes--

SENATOR HENRY: What is the most common way they get into our system?

MR. GERAGHTY: So, one thing, we do target -- or, bad actors target people. Because it's easier to hack a person than it is to hack a computer system. I can get you to open an email; I'm sure I can send one to all of you, and you'd open it. And, it could be malicious, and bad actors know that.

So, getting people to do that is easy. The education part that we were talking about is when you get something that has that sense of urgency,

that should be an alarm that goes off that maybe this isn't right. I don't need to change my password right away or I'm going to lose my account. There's something that should have prompted that. So, that's our job, to be able to educate folks on those phishing type of emails, or those laws that are coming in.

SENATOR HENRY: But, you're saying that's almost impossible--

MR. GERAGHTY: One hundred percent, yes--

SENATOR HENRY: --to take human error out of the equation, as--

MR. GERAGHTY: Absolutely.

Where, you know -- humans are fallible. As much as we don't like to think we are, but we're going to make mistakes.

SENATOR HENRY: And, you think advancements in technology would lessen the opportunity--

MR. GERAGHTY: Absolutely--

SENATOR HENRY: --for these successful cyberattacks to find -- have to find another way.

MR. GERAGHTY: Yes, absolutely.

There's lots of technical controls we could implement. Obviously, the detection -- being able to detect emails that are coming in before they get to a user's mailbox. Other things -- requiring strict access controls to the information that they need to have access to, rather than just blanket access to everything within an environment. Those are going to lessen and lessen the risk that we have.

SENATOR HENRY: OK.

Thank you very much.

Thank you, sir.

SENATOR GREENSTEIN: Senator.

SENATOR McKNIGHT: Hi; good morning.

Thank you for your testimony.

You mentioned that you have a number of instances, and then you report that out to the different entities. Are you following up with them to find out what they have done? Like, are you getting the information back from them so that can help you with a collective approach of, "Hey, these five entities have done X, Y, Z. Maybe we can dig deeper, and then we can educate other entities on implementing these particular policies?"

MR. GERAGHTY: In some cases, yes, we do get information back that they say, "Thank you, this was helpful." In other cases, it goes into a black hole, unfortunately. And, we don't get any feedback.

We do follow up in a lot of cases, but I know this morning we notified 22 organizations in New Jersey that had a critical vulnerability that is actively being exploited by threat actors. So, we will follow up with them as well.

SENATOR McKNIGHT: So, what is-- So, how many times do you follow up? Because I see that's an issue. If you're sending-- If you're sending entities that report saying, "Hey, look at this, because this is your -- you're the expert and they're not following up." So, do you follow up with them twice, three times? Is it an email? Is it a phone call?

Because, we need to really get to those entities because it's a potential harm to government.

MR. GERAGHTY: I think that depends on the criticality of the vulnerability, and the criticality or sensitivity of the targeted organization -- you know, how many (indiscernible) for follow up with them.

SENATOR McKNIGHT: OK, so maybe, through the Chair, we can look at that legislatively. Because, we should have some type of contact with them letting them know, "Hey, this is it. What have you done? Do you need help in mitigating this issue?"

And, the last question I have is, you spoke about international attacks. Do we have a number on attacks via -- through our country? *From* our country.

MR. GERAGHTY: So -- yes. And, the United States has the most sophisticated technological infrastructure in the world. Our internet speeds are greater than all over the place. So, it makes sense that threat actors from overseas are going to use cloud services here in the United States, or infrastructure in the United States, in order to carry out attacks elsewhere. That's just a natural use of getting the biggest bang for your buck.

So, we're seeing that all the time, and we're seeing that not just where they're using those cloud services -- or servers, if you will -- but home computers being compromised, unbeknownst to those users, or the owners of those systems, and then are being used to attack others. So, when I talk about China and Volt Typhoon, that's exactly their *modus operandi*, is that they are first hacking into a low-level individual, or a low-level organization, that doesn't have the resources to detect that, and then they're using that home internet or small office internet system to attack telecommunications and critical infrastructure here in the United States.

SENATOR McKNIGHT: OK.

So, just one last comment.

So, since you mentioned low-level, then we need to think about ways to reach out to small business owners--

MR. GERAGHTY: Everybody.

SENATOR McKNIGHT: Yes.

Thank you.

SENATOR GREENSTEIN: Thanks.

I was just going to ask you -- this is probably my last question, too.

There was a bill that we passed -- as I said, we have passed a few. This one was P.L.2021, c.19, and it was a Greenstein/Madden/Murphy/Benson. Requires public agencies and government contractors to report cybersecurity incidents to the New Jersey Office of Homeland Security and Preparedness, and it was enacted on March 13 of '23. That isn't *that* long ago, but has that bill been helpful?

MR. GERAGHTY: Yes. The incident reporting, as I mentioned, in 2022 -- prior to the law -- we had 96 reports from public agencies. In 2023, after the bill was passed, we had 141. So far this year it's actually 147; when I wrote the testimony, it was 146.

So, yes. Still, not everybody knows of the reporting, and the reporting was never -- and, I don't think ever intended to be punitive, OK. It was more -- it was the cyber neighborhood watch. If you saw a white van in your neighborhood and two guys got out with hoodies and they were trying to break into cars and stuff, you'd let everybody in the neighborhood know. That's what we're trying to do here, is we take that information and we put out bulletins, advisories, and alerts to those who receive them.

SENATOR GREENSTEIN: Great, I'm glad to hear that it was useful.

Does anyone have anything else? (no response)

OK, thank you very much; thank you for coming.

And, I know you submitted testimony, so thanks for that.

OK, so, now we're going to have Lieutenant Ryan Hoppock, Deputy Director representing the New Jersey Regional Computer Forensics Laboratory.

Why don't we also have Bill Kemnah -- FBI CART Certified Digital Forensic Examiner, representing the New Jersey Regional Computer Forensics Labs.

I think you could both come up.

Thank you.

MR. GERAGHTY: Thank you.

SENATOR GREENSTEIN: And, Lieutenant Hoppock, why don't you begin.

L I E U T E N A N T R Y A N H O P P O C K: Senator, Committee, thank you very much -- oh, sorry.

It's only my second time doing this; I apologize.

Senator Greenstein and the Committee, thank you for having us here.

I testified originally to this bill -- 2022, I believe. I stand by what I had said back then, and I'll give you a brief overview real quick, for those who don't know me.

I am the Deputy Director of the New Jersey Regional Computer Forensics Laboratory -- that is an FBI-administrated task force. The State

Police has -- New Jersey State Police -- has a unit inside of there, which I am the Unit Head for. Forty-eight percent of what comes into that laboratory is coming from the State Police, and about 48% is coming from the FBI, with the remainders coming from our counties. We handle a majority of the digital forensics evidence in the state. We're very lucky that we have our own laboratory for the state. It's a huge asset for us. Laboratories across the country -- there's 17 of them; there's 16 other laboratories -- those others share large geographic areas and are very busy traveling and receiving evidence from different places. So, we're in a great position to see the landscape as far as all criminal activity in the state, because--

SENATOR GREENSTEIN: This is located at the (indiscernible)?

LT. HOPPOCK: This is located in the Hamilton--

SENATOR GREENSTEIN: Oh, in Hamilton--

LT. HOPPOCK: --Township Technology Complex, next to the Troop C headquarters.

SENATOR GREENSTEIN: Yes.

LT. HOPPOCK: It has its own portion of the building.

So, we have this advantage to see a lot of what's happening in the state involving all types of criminal activity. Digital evidence is so prolific that it's pretty much in everything you can think of. I actually have a hard time finding or thinking of a criminal statute that I haven't seen, with some form of digital evidence.

So, with that, it also includes crimes that are involving cyber, in nature. So, we see a lot of activity related to not only crimes against children

-- which is both domestic and international -- but, also, intrusions and the like; investigations that are coming from both State and the FBI.

And, prior to me being at the lab, I was on the investigative side of this story, so I've spent about roughly 15 years or so either on the FBI's cybercrimes task force, or just solely with New Jersey State Police cybercrimes unit. So, these cases are not unfamiliar to myself and Detective Kemnah. I think that any type of reporting that we can gather from the public -- so, just echoing, on my own side, in my own way, what Mike Geraghty had said. Any kind of statistical gathering data sets that we can get that give us an idea of what the pulse is out there helps us allocate resources appropriately, but also helps us communicate effectively with our Federal partners. I can't stress enough that the relationship we have with them has really proven effective for a lot of victims, whether it be individuals or large companies that are falling victim to a myriad of crimes.

Now, the last thing I want to make mention of is that I hear the law itself we're looking at -- making some changes to it. I think that the way it stands right now, I just want to make it clear that it's absolutely been beneficial, I know, for the Federal partners that I work with often in cyber. They-- Multiple agencies have come to me and said that they've actually been able to use those datasets to collaborate what they see from their own threat intelligence, and it's helped them get more victims in their purview. So, victim notification is a *big* part of what we do. Attribution is very difficult; I've heard that theme. I think everyone in here is probably aware that international attribution -- holding people responsible for these crimes -- can be very difficult. But, sometimes, disruption of these groups is more of what the goal is, and having these datasets allows us to communicate effectively

where we're working at attribute activities together and make it known that we understand who it is that's committing what type of crimes, and target those groups and what -- and, get the information out. So, victim notifications are very important to tell people, "Hey, you may not have known that you were a part of this."

SENATOR GREENSTEIN: Before you go, I just had a quick question.

What's the difference in the kind of work that you do versus what Mr. Geraghty does?

LT. HOPPOCK: So, it's on the investigative side. Currently, right now, at the laboratory, we are in a supportive role. So, investigators, whoever they are -- Federal, State, local; mostly Federal and State -- conduct investigations of a variety of matters. When it comes to cyber, they may seize computers, cellphones, servers -- which are nothing more than just a computer implemented for that purpose. It could be drones; it could be anything that has digital forensics evidence. And, we will process that, and we will help support those investigations with the information we find.

So, as far as it goes in my history, though, I have been on both sides -- whether it be the digital forensic incident response side, or the actual investigative side, where we responded and sat in front of these victims -- whether it be an elderly, vulnerable community member in New Jersey or a C-suite about how they've been affected by a crime. Whether it's their systems are being misused -- so, leverage to attack someone else -- or whether they are the actual victim; whether they've lost, a lot of times, money, or they've lost control of their data, whether it's been exfiltrated -- for example, nation-state actors taking information from them.

SENATOR GREENSTEIN: Thank you.

Why don't you go ahead.

W I L L I A M K E M N A H: Good morning.

Thank you for having me.

My name is William Kemnah; I am a Detective in the New Jersey State Police, and I'm assigned -- this is my Lieutenant right here -- I am a detective within the task force, the FBI, at the Regional Computer Forensic Laboratory, which is right in the Hamilton Technology Complex. I am just coming up on 13 years on, so you have the older, more senior veteran who has been through it a lot longer than me, and then you have myself, who has just been through the training gauntlet -- over 400-something hours of training through the FBI as a digital forensic examiner.

I handle day-to-day investigations; I'm a boots-on-the-ground kind of guy, so if a call comes in and they need me to go investigate or go pull DVR footage, or we get a cellphone submitted to do digital forensics on, that would be me. I would handle that in the back of the laboratory.

Prior to being assigned there, I was down in the Cyber Crimes Unit for about four years. So, we would handle any investigation that came across our desk -- whether that be anything Federal, State, or local municipalities. Pretty much if anyone were to Google right now where to report a cyber crime in the State of New Jersey, that office phone would ring. We would have to mitigate any kind of questions that came through, saying, "Hey, I've been a victim of ransomware, or I Venmoed somebody $500 for a dog online and I didn't get that dog, how do I handle that?" And, we would help them to help do that. So, we can offer two different perspectives here on entry-level detective work, or different assistant directors.

SENATOR GREENSTEIN: Thank you; thank you.

Any questions?

OK.

SENATOR MORIARTY: Good morning; thanks for being here.

How capable are local police departments in New Jersey of dealing with cybercrimes?

LT. HOPPOCK: I'll take that.

Not very capable.

SENATOR MORIARTY: I didn't think so.

Is there a need to upgrade the training of local police departments to what may be the new crimes of the century that are going on *every single* day? Because, I am pretty sure if I called up my police department and said, "I've just been a victim of something on my computer here, and I just got taken, I ended up -- money is out of my bank account," they're going to say, "Yes, that's a civil issue. You should sue them," or something.

LT. HOPPOCK: Yes, Senator, the experience I have -- which has been a while; 23 years with the State Police, 18 of that in and around cyber -- those departments vary, quite tremendously, really.

There's-- We do the best we can without having an official mechanism to train and inform, and there are some great people out there. The NGRC (indiscernible), by the way, provides a lot of free training that law enforcement can sign up for. That helps them on the digital forensic side; not so much the criminal investigative side, how to handle those complaints that you're referring to. And, that is a weak spot in the law enforcement community for sure. Especially on the local level.

SENATOR MORIARTY: So, is there a need, maybe, for legislation mandating certain types of training? Because it seems to me that if I went into a local Wawa and said, "I have a gun in my pocket, give me a hundred bucks," and they gave me a hundred bucks, and I walked out, I'm going to get arrested and tried and the whole thing. But, if I call up my police department and say, "I just was the victim of a $10,000 scam through my computer," I'm not going to get any help.

LT. HOPPOCK: I'm not sure if the mechanism would be legislation. I wouldn't be-- I'm not saying I would be against or for that. I think that there's something that should be done -- *could* be done -- to enhance those--

SENATOR MORIARTY: But, why haven't they done it, then? If they're so-- It feels like we have-- I love our local police departments in my district; they're really good. But, if they're not up to the task of modern-day criminals, they need better training. And, if they haven't done it already, maybe we need to coax them a little bit? I don't know.

MR. KEMNAH: There are trainings available, depending on the detectives or the investigative unit or criminal investigation offices; free trainings online from NW3C, and things like that, so there's a plethora of training gauntlets. Maybe academies can be more influential in establishing a baseline, instead of just patrol tactics, or so on. I could definitely see recommendations going towards, well, this is now more vehicle; this cellphone is more deadly than a gun, because this can take down a whole network, like Director Geraghty mentioned. We are the weakest link in that equation, so crimes can be exfiltrated through any one of us. And, unbeknownst to us, we may have clicked on it by mistake.

So, training is definitely something we should push more towards.

SENATOR MORIARTY: How difficult is it for you to trace the perpetrators? For example, on a public network here today, and I'm running a VPN and it's going through Germany. Can you track what I'm doing?

LT. HOPPOCK: That depends.

SENATOR MORIARTY: On what?

LT. HOPPOCK: It depends on the nation-state that you purchased that service from; where the servers are. And--

SENATOR MORIARTY: Does it have to do with the nation-state where I purchased the VPN, where I'm paying them to be my VPN? Or, does it matter which nation-state the server is located in? Or, both?

LT. HOPPOCK: As I understand it, it's both, and it depends on where their infrastructure is located as well. If their infrastructure is located in the host country; if their business is, in other words, located in Germany.

SENATOR MORIARTY: This business is located in Romania. And, the server that it's going through is in Germany.

LT. HOPPOCK: It would-- I would-- I hesitate to speak too much on those issues, because--

SENATOR MORIARTY: I'm in trouble?

MR. GERAGHTY: You're in trouble. Don't trust (indiscernible) service providers in Romania.

SENATOR MORIARTY: OK.

LT. HOPPOCK: I'm glad that Mike said that, because I'm skirting the line here with how much can I let go.

I would say that I would not trust overseas providers at all. They absolutely will say one thing and do another. I know that firsthand.

SENATOR GREENSTEIN: Why did you get something from Romania?

SENATOR MORIARTY: I don't know, it just happens to be.

But, in terms of whether you can track what I'm doing, the answer is--

LT. HOPPOCK: It really depends. It depends, it depends on-- Using a VPN, for example, is one form of concealing one's activity. You're encrypting your data in transit, and then you're subjecting yourself to whatever controls and mechanisms that the infrastructure for the VPN company has set up.

So, if they're, in other words, logging everything you're doing, but telling you they're not, well they could be holding a record database that you're just unaware of that maybe someone has access to -- like the Romanian government for example, or whatever government. I'm not going to pick on a country or a location, but it is possible that there's more to the story as to your activity.

Tracing somebody is definitely not impossible. It takes a tremendous amount of resources, which is why datasets are very important. So, threat intelligence -- if we look at this particular law as threat intel, OK -- being that I'm from the State Police, I'll keep it limited to what I'm going to say about the Federal methodologies here -- but, they will absolutely draw upon different sources for threat intel.

And, when they do that, they'll make a decision as to what resource to throw towards it. And, oftentimes, there are many things that

you would think would not be able to be traced, and yet they are. It's just, when is it worth the time and effort? Because, it can be considerably high to do that.

SENATOR MORIARTY: So, getting back to training, I think you said there's online training, things like that.

Would it be best to maybe prescribe some best-practices training, as opposed to I'm taking some online course that I watch a tape for a couple of hours? As opposed to what is the baseline training that you should have if you want to be helpful to your community, as opposed to hit or miss -- I'm taking this training.

We all know that police training can be different depending on who is providing it. We found that out last year with some rogue police training down in Atlantic City that probably wasn't best practices. So, maybe we should have some kind of prescribed training.

LT. HOPPOCK: I would like to actually say that the first place I would start with that is mandating some form of digital evidence handling training at the beginning, and then, potentially, as a continuing education module for folks who are out in the field in uniform. That would be where I would start.

And, then, there's easily a way there where you could ensure order without burdening law enforcement without evermore training modules; giving them the information they need to direct citizens to where they can best get help -- best report their criminal activity and best get help.

Sometimes those folks do just need to have reports from the stations. I have found that that's, in my experience, been sometimes a trouble spot for people where they want to report something so they can get a copy

of that report for maybe insurance purposes, or to make some type of claim, and then there's an inconsistent-- The departments are basically making a decision, "Hey, we don't do that," or, "We do do that." It's two different degrees, so maybe there's some consistency there that could be very easy to have around.

MR. KEMNAH: I can speak to that as well, as far as my own experience as a detective. I've been a detective now for about seven years. Prior to getting that detective rank, we had to go to criminal investigation school, which is a two-week school, which is a gauntlet of all the assets we have available to us.

So, as the Lieutenant was saying, it depends on a lot of things when it comes to training and how it's offered. Certain local police departments only have 10-, 15-, 20-minute rosters where there's only one or two guys in the Detective Bureau. So, the general patrolman who is going to be going and responding to that call for service saying that they were taken advantage of, they may not have the training that was available to them because their PD isn't staffed accordingly for it.

So, it is definitely something more that is a challenge to try to push everyone forward, but some things that we're making ourselves available for. Like, we also offer -- which I'm an integral part in -- with (indiscernible) crime school, which is a subsidiary after you become a detective; you can put it for one of these other advanced training classes. But, it also depends on how hungry the investigator is and if they're looking to expand their own intelligence.

LT. HOPPOCK: But, not all of these opportunities would be available directly to locals. I mean, Bill is absolutely correct that most of

those are definitely available to State Police, and, even with that said, we see new members come in and there will be a lag time to getting the information out to those folks. And, it's not that-- It's a matter, I think, of maybe statewide having some consistency.

SENATOR MORIARTY: Thank you.

Your perspective on cryptocurrency?

LT. HOPPOCK: So, cryptocurrency, we have seen used quite often to be the means of transferring funds -- illicit funds -- specifically with ransomware. I have also, personally, had success with an investigation -- I'm not sure if I mentioned it the first time I testified here -- but it was an investigation I took to Federal court, and we did charge somebody for this. It was an insider fraud case where the individual was selling credentialed access to sensitive materials that a data analytics company had -- it's a large database, essentially, that was used for the purposes of creating insurance scoring, so they could score premiums for premium rates. A lot of sensitive information was in there.

Anyway, that person had put this up for sale with crypto. We actually used crypto in that case to lure the person out and get some proof of life -- what we call proof of life -- some photographs and stuff that was sent by the individual. I can't give too much away, but we were in control of those potential -- we used it as flash money, if you could use that term, as much as there is in the criminal world in narcotics, where someone is given money on behalf of the State and they show they have it to kind of prove that, "Hey, you know, I intend to do business here."

Anyway, crypto is interesting, because I think that it makes me think of what people don't know is that prior to us seeing crypto, we were

seeing gift cards used the same way. And, those gift card numbers, just being transmitted electronically through some type of -- whether it be a signal app or WhatsApp -- usually WhatsApp -- or text messages, or email, and then that money would be transferred much the same way that crypto is. But, crypto just adds a layer -- a greater layer -- of anonymity.

If we can't-- If we don't know what that wallet is, I understand there's many different types of crypto, and they do work differently, but there's a similar thread here is that it's giving some degree of anonymity to the person who is receiving the money if we don't know whose wallet that is.

So, we've had success. I know the Federal Government and the State both have some abilities to trace where crypto transactions go. But, we don't have control over these foreign markets. So, if money goes to overseas, we'll see it go there; that could be put into the space of threat intelligence, once again, if we were able to trace things down.

Crypto is an interesting thing. It's much like gift cards; we can use them legally, and then there's another way you can--

SENATOR MORIARTY: I take it you're aware that a-- I guess in the last couple of years, these Bitcoin ATM machines have cropped up. They're in gas stations, convenience stores, restaurants, you name it.

Is there any legitimate purpose to having a Bitcoin ATM machine?

MR. KEMNAH: I mean, there is. If I have a wallet, and I wanted to add funds, sure; someone could be using that in a legitimate way.

SENATOR MORIARTY: What's the likelihood-- What's the percentage of legitimate-- Would you venture a guess as to how much legitimate transactions take place at Bitcoin ATM machines?

LT. HOPPOCK: I wouldn't know the exact percentage, but I can tell you for a fact that I know that people conducting criminal activity have used those ATMs.

MR. KEMNAH: I mean, as far as cryptocurrency ATMs, I mean, it's just for a profit. Those people who have storefronts are putting them out there because they're taking insane profit off of the margin of-- You put in $100, you're not getting $100 of the Bitcoin, you're getting like $40 of Bitcoin; you're paying a service fee of 60%.

As far as cryptocurrency in general, yes, it's used in nefarious ways. But, a lot of people also, in today's day and age, are using it for profit and some quasi-investment even though it's deregulated and they never really know where it's going. People think it's up on certain applications where you can do it from your phone. People think -- especially younger communities -- they think it's an investment opportunity; it's going to go through the roof, and they-- So, there's a different allure to it as well.

But, as the Lieutenant was saying, if a nefarious actor is looking to seek profit or gain from a scam, they're going to use any which way they can. This decade it's cryptocurrency, but wire transfers have always been around; banks hung their hat on not complying with them after they're sent because you signed the paper that says, "Yes, I want to buy or transfer $100,000" to my Lieutenant. Meanwhile, I didn't know it was a scam. The banks will go, "You told me to do it, so I'm out of this," and if you don't execute that 72-hour kill chain to get that money stopped in its tracks, it could be wired overseas and then lost forever.

So, gift cards are a thing, too, especially around the holiday season. People go in and they cut the top of the gift card off, meanwhile you

go activate it at the register and it comes in. Meanwhile, a gift card has no actual money; this person who left the store already has top of the gift card.

It's just -- you've got to stay current in education, and training is key.

SENATOR MORIARTY: Thank you both for being here.

SENATOR GREENSTEIN: Senator.

SENATOR MCKNIGHT: Yes, just-- Thank you so much for being here.

I'm just listening to the questions that the Senator just asked.

I want to know, do you feel that the police department should create a special cyberattack unit? So, this is where there are designated people -- law enforcement officers -- who can handle the call, such as the Senator said. You know, I got an email; I clicked on it; and now I'm out of $10,000. Because normally you would call, like, the non-emergency number to say that.

So, my question to you is, should the police department create a special cyberattack unit -- such as we have IA, and we have a special unit. Should we have that, especially since cyberattacks are on the rise, and this seems as if it's even higher?

And, I'm thinking -- I believe Michael said it earlier -- we need to think forward, and not just being reactive; we need to be proactive. So, you can just ponder on that question.

LT. HOPPOCK: I think when it comes to the most vulnerable people in the state, I think of the elderly immediately when you say this. It's not just people of that age, but that group is -- has been -- very much targeted. And, they're -- it's very common to see those reports. And, we know of

reports that maybe don't funnel them right to the cybercrime unit at the State Police.

I don't know, other than the Internet Crimes Complaint Center -- *ic3.gov*, which is administered by the FBI -- I don't know of any other reporting mechanism that's out there. There may be, but people -- victims of what you just said, where they click on, and they'll -- they can submit there. It's not-- There's no obligation; it's voluntary.

So, as far as creating-- Is it law enforcement that would be best serving the public in that instance? I would think in-- I would think in this setting, I would say I don't think that's necessarily the step that's going to be the most effective in getting those people help. I think it's having a place for them to report, and then having resources dedicated to look over those reports, and treating them both as threat intel. And, also, as -- where can this -- what law enforcement agency can talk to these folks to help mitigate this? Because there could be, if it's reported fast enough-- In the case that you described, it's not really much of an oversimplification, clicking on something or agreeing to send money. It has to come from a financial account.

The faster that gets reported to law enforcement-- In our experience, Bill and I know this very well. If we know that this happened within 24-48 hours, we can activate what's called a financial kill chain. The difficulty we face is the communication with the banks. There is no one line or one repository for us to go to, to go to whatever bank and say, "Hey, this just occurred, we want to try to stop these funds from being completely transferred."

SENATOR McKNIGHT: Yes, but this is a crime, right?

LT. HOPPOCK: It is, absolutely--

SENATOR McKNIGHT: Let's look at an elderly, losing $15,000 out their bank account. And, that $15,000 is to help pay for caregivers. And, a senior would call 9-1-1 -- "Wait a minute, my money is gone."

So, instead of telling the elderly, "Oh, this is a civil case," my question is, should she -- should the elderly be transferred to a designated unit so that they can take her -- or, his or her -- information, and then push it, transfer it over to the right authority? Because, if I'm calling, you're telling me this call -- this is a civil, where I'm like, "OK, what am I going to do here? I just lost $15,000."

So, my question is, should we have a designated department who is trained -- not on YouTube, but who is really trained to handle and mitigate these matters? Meaning, maybe they are going to call the State; maybe they are going to call the FBI, versus just talking to the dispatcher.

LT. HOPPOCK: It is. You've got to forgive me there, it takes me a little while to come back around, because having lived in the reality of it, I immediately go to what are the speed bumps, the road blocks.

I'm not against what you're saying. I actually think that's probably not a bad idea, because you're-- I like the efficiency of that idea. Especially when it comes to what I was -- where my head was going with trying to help these people if they call us soon enough. And, then, the difficulties we face trying to get that money frozen to get it back. Because it often does go overseas, or it goes through several hops, just making a complicated trail that we can't unravel.

We've had a lot of success, though, in the past getting monies returned. But, yes, if there was a way to shorten the length of time from the

initial, “I call 9-1-1 because that’s what you do,” to, “OK, you have someone from the cyber crimes unit, for instance, at the State Police who understands what just occurred -- great.” Because, then that time has shortened that we can activate the kill chain.

SENATOR McKNIGHT: Thank you.

LT. HOPPOCK: Welcome.

SENATOR GREENSTEIN: Thank you.

Senator.

SENATOR HENRY: Yes, thank you, Chairwoman.

I have two questions.

First, understand the magnitude of what’s going on with these crimes. How many of these crimes do you believe go unreported -- out of embarrassment, out of, “Hey, I’ve been taken, I’d rather not say anything?” People are embarrassed sometimes when they get taken with these scams.

Do you have any idea how many are not reported?

MR. KEMNAH: It’s really difficult to tell (indiscernible) with that. I mean, I would say a lot. I would be willing to bet 50%, depending on the severity, how much that person had financially, if it’s that big a hit. Or, like you said, if it’s linked to something nefarious, or like the extortion scams that go on, saying, “I’ve witnessed you doing something nefarious online and I want you to send me $1,000 or else I’m going to release these photos of something.” It comes to a factor of that. So, yes, it’s kind of hard to tell exactly how many--

SENATOR HENRY: The problem is bigger than a lot of people realize.

MR. KEMNAH: Absolutely.

SENATOR HENRY: And, my second question is, should someone report an incident to you? How many times is there a positive outcome, percentage wise?

LT. HOPPOCK: There's no official statistic on that. It depends on what type of crime we're talking about, and where do we get -- where are we getting-- So, when I specifically talk about the investigative side of things, Senator, I'm talking about my experience in the State Police Cyber Crime Unit.

It's very difficult to generate work there if you're not going to look for it. People do occasionally cold call in, and it ends up being a good case, so it's hard to get a statistical number as to what's going unreported.

There's a lot of material that we'll look through in order to find something that actually has traction to it. *IC3.gov*, for example, is a good website where people self-report. And, it can be even difficult at times to find out where those people are actually living, because they will fill a form out as if they're here, and they're not. There is no way for us to really know that, given what the current state of that reporting mechanism is.

SENATOR HENRY: I've been involved in a few cases, and, fortunately, with our town -- when our town was a transfer, and it contacted the Prosecutor's Office right away, and, thank God, overnight the town was able to stop that transfer, and it happened.

But, I've seen so many where our local police department were investigating, and they hit a dead end. They take it-- The larger departments have the ability to look into these matters, but some of the smaller departments don't. So, I've just seen it both ways, where we've been successful and where we have not been successful.

MR. KEMNAH: Each investigation--

SENATOR HENRY: (indiscernible) relief--

MR. KEMNAH: Every investigation is going to be separate. I mean, sometimes, with today's day and age and privacy and encryption and a timeframe of executing warrants and subpoena results and getting results back and then following that up, and as the other Senator's question with the VPN services, you can track down certain hops.

So, in today's day and age, in an era of privacy, law enforcement is up against the wall with that, and we're seeing it at the very end of the result that that's what happens. We don't know how long it took to execute that whole thing. So, if we sent a warrant out here, it may result in these results, but then we have to spend another warrant out here, and getting that back in a timely manner.

So, sometimes you have to deal with dead ends, or it goes overseas, or it goes to a jurisdiction that's not complying. Or, they say, "We don't have any data on that; we can't comply with your request because one, we're outside of the jurisdictional lines in the U.S., or no one told us we have to keep that data, so we didn't store that data." So, your (indiscernible) here.

So, unfortunately, it depends on each investigation. There has been fruitful ones where full bore, we get our money back and then we execute and seek prosecution on the individuals, and there's some that we have to then transfer over to another jurisdiction.

SENATOR HENRY: I look forward to working with everyone to try to get some type of legislation proposed and passed that would help make -- help improve the situation.

As you know, I have the victimization bill out there that would make these crimes against seniors -- as you said -- who seem to be a prevalent target. Bring it to the next level, that they have additional penalties be assessed against them, should you be successful in finding these people who target seniors.

I thank you for being here today.

Thank you for what you do.

LT. HOPPOCK: Thank you.

MR. KEMNAH: Thanks.

SENATOR GREENSTEIN: Thank you both very much, we really appreciate the testimony.

Thank you.

LT. HOPPOCK: Thank you.

SENATOR GREENSTEIN: So, I think we're all set. Thank you.

Now we're going to have Mark Musella, Bergen County Prosecutor, and Lieutenant Christopher Whiting, Intelligence and Counterterrorism Unit of the Bergen County Prosecutor's Office, representing the County Prosecutors Association.

Thank you.

M A R K M U S E L L A: Good morning, Senator Greenstein--

SENATOR GREENSTEIN: Morning--

MR. MUSELLA: --Greenstein.

Good morning, Senators.

Thank you for having us here this morning.

My name is Mark Musella; I am the Bergen County Prosecutor.

I brought with me today Christopher Whiting. He is the Chief of my Intel and Counterterrorism Unit.

Should I start again? I'll start again.

Good morning, Senator Greenstein; good morning, Senators.

Thank you for inviting us here this morning to speak on this issue.

My name is Mark Musella; I am the Bergen County Prosecutor.

I brought with me this morning Christopher Whiting; he is my Chief of our Intel and Counterintelligence (*sic*) Unit. He also oversees and works on a daily basis with our Cyber Crimes Unit, our Financial Crimes Unit, and our Digital Forensic Lab that is located within the Bergen County Prosecutor's Offices in Paramus.

I have a brief statement, and then I am going to defer my time to Lieutenant Whiting, who I believe is really an expert in this field and those of many of the people in the room who testified this morning.

As we've heard this morning, counter-- Strike that.

As we've heard this morning, cybersecurity must be one of our top priorities. We must all be -- we must all remain cyber vigilant. Cybersecurity threats are one of the biggest threats business and government face today. We must view cybersecurity as a continuous game of security, and we must view it as a team sport, and that we must continuously partner with our government agencies, our public and private partners, to stay one step ahead of the attackers.

And, we can do this through funding, education, and the sharing of notifications, reports, and information and resources. We must stay ahead of new threats -- new threat trends as well, such as the use of AI to make

cyberthreats and ransomware and malware more difficult to detect. We must also be aware that we can use AI -- specifically generative AI -- in the defense of cybersecurity threats as well.

Finally, all critical-infrastructure cybersecurity threats should be reported, because the more we partner and share information, the more notifications that we make, the better we can protect our networks. And, that's really the goal, is to protect our networks against these cyberattacks, and we believe that the sharing of information and the partnering is really critical in this regard.

I'll be available for questions as well, but, again, I'll defer to Lt. Whiting.

LIEUTENANT CHRISTOPHER WHITING: Thank you.

Good morning, and thank you all for having us; I appreciate it.

To echo Director Geraghty, my colleagues at State Police, and the Prosecutor's sentiments, I think that in listening to the questions from this panel, I would tell you that it just boils down to one piece: And, that is, this is definitely a team sport.

When we talk about cybersecurity, it is all-encompassing. Whether it be government or private sector, we all have to be on the same page. When we talk about training, unfortunately, there are only so many trainings we can roll out. A lot of this dives into expertise, and that's where it's critical. We're partnering with our state agencies, our county agencies, and our private sector.

The Director spoke earlier here about the NJCICC. For example, our agency, we oversee 71 law enforcement agencies. We partner with the

NJCICC; we partner with other organizations, such as the MS-ISAC, which is a private sector, Multi-State Information Sharing Analysis Center for cyberthreats. So, when one agency is getting threat actors or known actors, we're receiving that information and, at the same time, we're reporting that information out to the State.

In our jurisdiction, we started offering cyber surveys to our 71 law enforcement agencies in the hopes that our expertise could help them with vulnerability assessments on their networks. But, the landscape is drastically different in each of these places, and it comes down to not only expertise companies; software; funding; maintenance agreements; the myriad of different appliances out on the networks; all plays into this role.

I am available for questions as well.

SENATOR GREENSTEIN: Thank you.

Have you had any very big incidents of some kind of hacking, or other kinds of cybersecurity incidents that have happened in Bergen County? And, how have you handled them?

LT. WHITING: So, the answer is yes. We've had numerous. And, it depends on the type of situation. So, from our healthcare sector, we were subject of part of an ongoing ransomware attack last year. We've had some reporting from private sector, but mostly government reporting to our agency. And, through the Prosecutor, we offer assistance to those agencies for recovery and mitigation strategies so that we are not affecting more users.

It could be malware; it would be ransomware; phishing attacks. As AI gets better, the phishing attacks to our emails get more sophisticated and better crafted. And, they're harder to detect. So, when we talk about questions about training and pushing it out and trying to cover down on that

section of it, it becomes very challenging, because we are all fallible; we do read it, and they're getting better and better at it. So, the more that we learn to recover from this or to detect it quicker, we're better suited.

And, we've had that happen in numerous PDs.

SENATOR GREENSTEIN: Do you have any suggestions for what we can do legislatively to help here?

LT. WHITING: I would say definitely reporting with critical infrastructure partners is key -- and sharing that information.

I don't know, necessarily, how that rolls out countywide. I think that when you talk about the disparity of agencies' size in law enforcement, I think it's going to be left to the larger agencies or the county agencies and the State agencies to really mitigate those strategies. Because, again, you're talking about getting subject-matter experts. When the Prosecutor spoke about how our makeup of the office -- we have a Cyber Crimes Unit, that would be your normal detective rollout of whether it be child abuse material, or supporting an investigative squad to our digital forensics lab, similar to what the State spoke about with the Federal partnership, to our Bureau of Information Technology.

When we roll it out, it's a whole bunch of resources, depending on the problem. It's not just one group. So, it's not just detective staff; it could be IT professionals that have network administration backgrounds, or who handle our firewall or our intrusion detection systems.

So, again, getting that ecosystem -- the totality of it to respond to the incident.

MR. MUSELLA: And, just -- to follow up -- one of the senators have asked a question before about when something is reported to the locals.

So, in Bergen County, we have 70 towns. So, the local police departments -- the 70 police departments -- are really not well-equipped to handle certain cyberthreats or cybercrimes. They'll take the initial complaint and they'll do the initial investigation, but we encourage all our towns -- we meet monthly at our Chiefs meeting -- and we encourage our towns to call our office and really to connect with the expertise that we have.

So, we have -- *everything* runs through our Cyber Crimes Unit now, whether it's a homicide, a sex crime; whether it's a cybercrime or a financial crime. We leverage Cyber Unit, we leverage our Intel Unit, our Financial Crimes Unit works as well, and then our Digital Forensic Lab there -- that's where we really will be able to do the digital downloads of phones and computers and stuff like that.

And, I know Chris wanted to talk about encryption, so I'll make sure he gets to talk about that before we leave.

But, just so-- For example, if someone calls in and says that I had -- I've been a victim of a cybercrime -- let's just take a crypto, because we've seen a bunch of them in Bergen as well -- the local police department will take that initial complaint, but we urge them to call us as soon as possible, because time is of the essence. And, again, we have the expertise in our office to really -- to investigate those matters more thoroughly and fully. So, a matter like that would maybe go to the financial crimes -- the detective of financial crimes -- and we're working with the local police detective to try and put a freeze on the bank account -- so, a freeze on the crypto account, or whatever we may -- what we can do.

And, we've been successful in getting cryptocurrency; seizing -- freezing Bitcoin account and getting that cryptocurrency back. We've had

instances where the money went overseas, we seized the account; the perpetrator is overseas, he puts a little bit back on the block chain, or whatever the exchange, and we seized it. And, so, then he keeps the majority and then sends it somewhere else. And, we've had a case where $80,000 was taken. The actor put -- again, it was through a Bitcoin machine. The money was deposited in a Bitcoin machine; the money went overseas; it was an actor in India. We froze the exchange, but he was able to get the money off before that. And, when he puts the money back on, we were able to seize that money. But, then he realized that, and the majority of the money moved onto another exchange. And, there's so many, I guess, unregulated exchanges in Europe. But, that's a typical incident where our Cyber Crimes Unit, working with our Financial Crimes Unit, moved fast to help that victim of that type of crime.

So, I mean, we see those type of -- the things that we have always seen where people who are trying to scam people through the computer; through cellphones; in-person. But, we did have a breach -- I guess -- a security breach at one of the area hospitals, which I think went to the Senator's question.

SENATOR GREENSTEIN: OK.

Questions?

Yes.

SENATOR MORIARTY: I agree, speed is of the essence.

Are local police departments calling you?

MR. MUSELLA: Yes.

SENATOR MORIARTY: They are. So--

MR. MUSELLA: We encourage, in Bergen County, a partnership. We work hand in hand with our locals, and we advise them to call all the units we have that have expertise, to call them immediately; whether or not we can help them or not. And, they do call.

SENATOR MORIARTY: Because, when you talk about speed, if someone directs you to go to an ATM Bitcoin place and put in $10,000 -- which, by the way, happens every week--

MR. MUSELLA: Every day.

SENATOR MORIARTY: --every *day* in this state. People are walking into independent gas stations and putting $10-15,000 into these Bitcoin machines. That money is sitting there in that machine. Someone has to come pick that money up, you can intervene--

MR. MUSELLA: But the money-- But, it's much like wiring money, Senator. The money is gone; the money is an instantaneous transaction. That's the beauty of Bitcoin--

SENATOR MORIARTY: No, but they're putting cash in--

MR. MUSELLA: I understand that.

SENATOR MORIARTY: But, the cash is there--

MR. MUSELLA: But, that's not your cash anymore. That cash has been wired to a person in India.

SENATOR MORIARTY: But, that was done by the--

MR. MUSELLA: Exchange--

SENATOR MORIARTY: --ATM exchange. They still have the money sitting there in the bin, and you can take that money.

MR. MUSELLA: The money can be seized. But, again, the money now -- the money is -- it's sort of when you go to the bank and deposit

money in the bank, and that money is wired to a third person. That's not your money anymore; that's not the bank's money anymore. It's the third person's money. And, that's what happens.

SENATOR MORIARTY: No, I get it, but--

MR. MUSELLA: That was-- And, the problem is, again, with some of these transactions, they're voluntary. The person voluntarily puts the money in the machine, so there's no fraud that's been committed. The fraud is being committed by the person who receives the money on the other end -- in the other country, or sometimes in this country as well, but--

SENATOR MORIARTY: But, these exchanges -- the people who own these ATM Bitcoin machines -- they know, they see the flow. They see what--

MR. MUSELLA: Senator, it's like anything else. The machine is also used to conduct legal transactions--

SENATOR MORIARTY: Very, very limited--

MR. MUSELLA: Well, I can't testify to that, but it's like an ATM machine. You put your money in there, it's a transaction--

SENATOR MORIARTY: It's not anything like an ATM machine. ATM machines give people money -- these only take your money.

MR. MUSELLA: I'm not familiar with the Bitcoin machines. I know that they -- again, it's a machine that somehow you can either deposit cash into it to put into your own wallet, your own account, or you can use it to send to someone else to conduct the transaction. And, like anything else, it's subject to fraud or mal actors, we call them, or people who are out there scamming.

We had-- We had done a public service announcement on Bitcoin machines. We, through our website and our Instagram, we're always doing PSAs with regard to scams that are perpetrated on seniors. I personally go to senior centers; I've presented to over 50 senior centers on senior scams, especially around the holidays. In fact, today, we're putting out a PSA on a cybercrime that is a trend. I guess for the holidays, don't-- If you get a package on your front porch and it has a gift card in it, if you scan that gift card, it will download ransomware to your telephone -- to your iPhone -- so the person can get access to your passwords and personal information.

And, also, I believe the other one is-- One is there would be a gift card inside, and then the other one, there will be a QR code as well on a card to scan. And, that may give an actor access to your passwords and your personal information on your cellphone. So, don't do that.

SENATOR MORIARTY: Do you believe that we need to do more training for local police departments? Because, if you got every single scam to your department, could you even handle it?

MR. MUSELLA: I think training is always good. In each department, the way I understand it, there's a detective bureau in each of our departments. Those are police officers who have more time on -- more service time. Also, have more training and education. And, they're usually, again, detectives who have been in the department five to 10 years. But, those detectives are instructed to call our office, because we have the investigators who have the training and education and continuously deal with these type of crimes on a daily basis, and also continuously go for in-service training and continuous training and education.

So, again, the way it works in Bergen -- we get 11 homicides a year, but we have 70 towns. So, Alpine may get one homicide every 20 years. So, call us, because we're dealing with 11 a year, and our investigators are trained, educated, and have the experience and deal with it on a daily basis.

So, I think -- from a funding standpoint -- I don't know you get -- respectfully, we'll get all the 70 detectives in the 70 towns up to the level of people in our office. I don't think that would really happen. So, I think the funding should go toward the Prosecutor's Offices, so they have the units that are staffed; have the resources; and have the funding and training education and experience. And, that's the model we have in Bergen.

SENATOR MORIARTY: Thank you.

SENATOR GREENSTEIN: Yes, Senator.

SENATOR McKNIGHT: Thank you for being here and for your testimony.

And, just listening-- You're making my case, my recommendation, much stronger. I do feel that we need to have a special unit.

You mentioned that you urge--

MR. MUSELLA: We do, like I said, we--

SENATOR McKNIGHT: I mean for locals. You're saying that you urge police, you advise police, to call into--

MR. MUSELLA: Our office--

SENATOR McKNIGHT: --to your office when this happens. I feel that it should be mandatory, and there should be a policy where there's -- I'm now just using 24 hours, but it could be less. You have-- If someone calls into the local police, within 24 hours, they should be calling you.

So, I feel that we need to have a policy and procedure in place to help. Because cyber attacks are happening; they're happening.

MR. MUSELLA: Yes.

SENATOR McKNIGHT: And, it seems like they're not going anywhere.

And, also, in reference to the subject-matter experts with the training, do you have-- On your website, do you have a list of trainings that you recommend that the local police should take?

MR. MUSELLA: I don't think it's on our website, but I think-- All 3,000 police officers in Bergen County have to go for in-service training every year, and those trainings are at the police academy in Bergen County, which we also oversee. And, I believe my Chief puts out the trainings that are available. There are certain things that are required, but there's also other electives, if you will, that they can take. I don't know that cybersecurity is one of them. I don't know if Lieutenant Whiting can help me with this.

LT. WHITING: I'll speak to that quickly.

We put out more of awareness training for that level, so they can recognize and identify what is going on so that they know what resources are available for them to call. And, we're very proactive with that education piece, but it wouldn't be bringing them to the level of network intrusion.

And, when we roll it out, it's not just detectives. It could be our civilian staff that are part of our Bureau of Information Technology, because they're the ones who hold the card for the -- for that subject matter that we're looking at.

SENATOR McKNIGHT: So, how do you put the awareness out there? Again, is it an email?

LT. WHITING: For us-- For us, it's a little bit of-- It's multifactor. It's in-service training that we host, and we have regional detective meetings. So, they would get that information through those venues. We don't put it out publicly; some of the training that even was spoke about before our testimony from other colleagues are behind law-enforcement-sensitive secure databases. So, even just to access that training, you have to be a vetted user. So, it's not something you can publicize.

SENATOR McKNIGHT: OK, so-- But, do you have a list of mandatory trainings for locals to take? To keep abreast as to--

LT. WHITING: We don't. We don't have a list of mandatory, no.

SENATOR McKNIGHT: OK. That's something we should definitely look at.

Thank you.

SENATOR GREENSTEIN: Anyone else? (no response)

OK, thank you very, very much. I really appreciate it.

LT. WHITING: Thank you.

MR. MUSELLA: Thank you.

SENATOR GREENSTEIN: OK, and now we're going to have Robert McQueen, Director of Information Technology, Franklin Township, Somerset County; Past President of the New Jersey Chapter of GMIS International; representing the New Jersey League of Municipalities.

R O B E R T M c Q U E E N: Good morning, Madam Chairman *(sic)*--

SENATOR GREENSTEIN: Good morning--

MR. McQUEEN: --and, thank you for this opportunity.

And, distinguished Committee members.

Local governments face mounting cybersecurity challenges with limited resources and restrictive procurement rules that can actually increase their vulnerability. Further, critical cybersecurity reporting requirements and State communications aren't reaching the right local government officials, potentially exposing vulnerabilities. There's an awareness gap: Local officials, often unaware of cyber incident reporting requirements; limited outreach about reporting obligations; and communications frequently miss key security personnel.

Scattered State communications create risk -- multiple State agencies sending separate cybersecurity requests. We need to centralize all cyber communications through the NJCCIC. Current systems create confusion and security vulnerabilities. The biggest risk is public exposure. DCA's best practice inventory requires public discussion. It forces municipalities to reveal security measures, like MFA -- multi-factor authentication -- stats.

Published council agendas and minutes can give threat actors intelligence about local government vulnerabilities. What's needed: A secure, centralized communication channel; route all State cyber communications through the NJCCIC; better outreach and reporting requirements; and, protected method to share sensitive security information.

When it comes to cost, municipal cybersecurity costs are rising 10% or greater annually, against a 3% appropriation cap, while insurance requirements keep getting stricter. *All* cybersecurity-related expenses need to be outside of that 3% cap. An example: One mid-size municipality of 350 employees spends approximately $270,000 annually just on cybersecurity hardware and software. That breaks down to $771 per employee, per year,

for basic security. The total software budget for that municipality is $972,000, excluding police department.

Key challenges: Procurement rules create security risk. Public bidding requirements expose security details to potential threats. We need a confidential procurement process for cybersecurity purchases. Insurance drives cost and requirements. Insurers mandate specific security controls. Requirements consistently involve with technology. Each agency has unique risk profiles, making standardization difficult. There are hidden costs which also pile up. There's physical security; server licensing; staff training; log monitoring; access management; and inventory control systems. Staffing gaps create vulnerabilities. Most municipalities can't afford dedicated security experts.

Critical positions, like a Chief Information Security Officer -- or a CISO -- remain unfilled. The solution is State-level support, which could help. The NJCICC *could* provide a shared CISO at a county level; create an incident-response task force, similar to North Carolina's model; and support local governments during cyber incidents. New Jersey GMIS is working to create a volunteer response team, but a State-funded program could provide more reliable support. Without changes to funding, structures, or State support, municipalities will continue to struggle to meet cyber -- rising cybersecurity challenges.

I am open to your questions.

SENATOR GREENSTEIN: Thank you.

Anyone have any here? Any questions? (no response)

Senator? Any questions? (no response)

I don't either.

Thank you very much.

MR. McQUEEN: Thank you.

SENATOR GREENSTEIN: I really appreciate it, thank you.

And, I'm sure we'll get in touch with you privately for additional ones, which probably will come up.

Thank you.

OK, now we're going to move to the private sector. And, there are six people to testify. And, I'd like you to come up in groups of two, so it'll be like three panels.

The first person is Kyle Sullender, Director of Economic Policy Research, New Jersey Business and Industry Association; and, Neil Eicher, Vice President of Government Relations and Policy, New Jersey Hospital Association.

And, we can start with Kyle.

Wait a minute, you're not Kyle.

C H R I S T O P H E R E M I G H O L Z: (laughter) I am not Kyle, Kyle--

SENATOR GREENSTEIN: I can actually see that. (laughter)

MR. EMIGHOLZ: Kyle, unfortunately, is under the weather this morning; woke up with a fever, and does not want to get anybody sick. And, so, he chose not to come to the State House. So, I am covering for him.

His testimony should have been emailed to all of your addresses, so you should have it -- the Committee should have it.

So, thank you very much for inviting NJBIA--

SENATOR GREENSTEIN: Say who you are.

MR. EMIGHOLZ: Yes, my name is Christopher Emigholz; the Head of Government Affairs for the New Jersey Business and Industry Association.

And, thank you for the invitation to speak about this important issue.

Basically, BIA wants to break this down into four key areas: Number 1: Cost. This is something that every business is facing, large and small. Since COVID, we've seen reports that these incidents have doubled in the private sector. We've seen statistics that the average entrepreneur is spending $8,000 a year on cybersecurity issues. We've seen estimates from national cybersecurity lines that a business that has a cybersecurity breach are probably going to spend $3 million to deal with it -- in the 500-range type business. So, obviously, there is a cost, and it hurts businesses all across the board.

Number 2 is businesses are actively, every single day, all across the state, large and small, dealing with this. There is a lot of best practices that we're doing, and I'm sure all of us have been -- (indiscernible) we've heard this before -- some of those trainings, "Don't open this email," gotten those emails from, whether it's State employers, government employers, or private employers, sending those emails to just check with your people. Could be more vigilant with that, and I have some ideas later on what the State could do to support that. But, we're doing that.

Number 3 is workforce development. This is an issue, and workforce development -- it's kind of an internal workforce development; external workforce development. But, the State needs to do more to support the employees who understand this -- because not every employee does, and

we still have those rates, as Senator Moriarty rightfully brought up, that are worrisome; that people fall for some of these scams out there and cybersecurity issues. And, a lot of times, no matter how much you do as a company to make sure that the hardware and software is protected, it's a human element, and you've got to train the people to make sure that they're not falling for these things. So, that comes training, so that's the internal workforce development -- make sure your people are prepared for these cybersecurity threats.

But, also, the bigger picture workforce development, I would argue, that we should invest in -- we already have, we should continue that -- is the external. We've got to make sure that cybersecurity IT professionals -- it's only growing as a great career in New Jersey, and we should make sure that New Jersey can be a place where we're leading on IT; that we're leading in innovation. I think we've seen innovation efforts recently by the Legislature and Governor that should be applauded; those should continue, and workforce development is probably the most important thing for innovation, and cybersecurity is a big part of that. The Pathways Program that the Legislature has funded for a few years in a row, that the county colleges and BIA have partnered on; IT, cybersecurity, is an element of that, but we've got to make sure we produce more people out of our high schools and colleges who are ready to go into careers in this area, and so that will not only help our State be ready, but it will also be a source of an economic growth for our State.

Lastly, I want to talk about manufacturing. We actually have a very heavy sector of manufacturers that do a lot of work for the Department of Defense. And, I don't have to say it more to our Chairwoman of the

Manufacturing Caucus, who is the Chair of this Committee. But, Senator Greenstein knows well, and she's heard, MEP has a program to help get manufacturers trained for the cybersecurity and certified, that they need, but we should do more to make sure that our manufacturers and anybody who is engaging in business that requires certain cybersecurity credentials gets those.

And, so, I guess things I would say to the State is we do a lot already; we heard some of the things we do. The Business Action Center has put on cybersecurity webinars for businesses. Lots of businesses -- and, I'm sure some might come up later -- do things for their members. But, I would argue, is there something we can do to consolidate the good work that the EDA; the Business Action Center; the Secretary of State; the Office of OIT does, and make sure that it's a little more of an easy-to-read access package for all businesses?

Number 2: Is there things that we can do, such as grants for those manufacturers, or anybody who needs these certifications? And, the last one is a hard one, because Legislature -- we want to do some things. But, sometimes, this is a -- not a State issue, not a local issue, this is often a Federal issue; sometimes it's an international issue. There's only so much we can do. And, so, sometimes when the Legislature tries to regulate, it becomes something that makes New Jersey an outlier and becomes more cumbersome, but it's actually not going to get at the problem, because the problem is an international one. We can't stop what a country in Europe or Africa or Asia is doing, and yet we're actually hindering what companies in New Jersey do because of that attempt to try to deal with what is a real issue -- but, sometimes, we have a tendency to overregulate sometimes. And, so, I just ask for caution on that.

But, this is a real issue.

Thank you for bringing us up, and we look forward to continue to work with the Legislature on ways to help our businesses with this.

SENATOR GREENSTEIN: Just a quick question: Is the private sector hooked in with NJCCIC in some way? Are you involved with any of that that we just heard from the public sector?

MR. EMIGHOLZ: I would not be the best person; I think the person who previously testified would.

But, I know there are some businesses that are working with the State on this. But, yes, certainly, could it be more? I don't know. My guess is there's always more room for public-private partnerships. But, I don't know the extent of that.

SENATOR GREENSTEIN: OK.

Why don't you have you finish, and then we'll do the questions.

Thanks.

MR. EMIGHOLZ: Thank you.

N E I L E I C H E R: Good afternoon.

My name is Neil Eicher; I am the Vice President of Policy at the Hospital Association.

I echo what Chris said; thank you for holding this hearing. And, it's been terrific listening to all the presenters so far.

I just have a brief statement, but there are a couple of issues that I want to focus on.

So, as we have been discussing, cyberattacks have been growing over the last couple of years -- in particular in the healthcare sector. Recent data indicates 128% surge in attacks in healthcare -- in the healthcare sector

-- from 2022 to 2023, and early indications in 2024 they're continuing to go up. This trend underscores the urgency of addressing vulnerabilities across the healthcare ecosystem, including not only hospitals, but also third-party entities. And, what I mean by third-party entities -- these are remote patient-monitoring apps; these are vendors that hospitals contract with; these are healthcare claims databases or processing units that health insurance companies use. These are third parties that hospitals are either required to contract or choose to contract with.

So, one example of this happened in February, with the Change Healthcare attack, which is owned by UnitedHealth Group. And, in February, this was the largest cyberattack in the healthcare industry ever, and it occurred in February. This attack disrupted critical hospital functions, such as claims processing; pharmacy operations; and real-time eligibility verification. The financial repercussions of this were severe, with claim submissions dropping by $6.3 billion for affected providers in just the first three weeks. Hospitals struggled to maintain operations; pay staff; procure essential supplies; and ensure patient care amid reduced cashflow and increased administrative burdens. For some, claims disruptions lasted over 60 days, straining resources and operational capacity.

Now, hospitals are required under Federal HIPAA laws to maintain certain cybersecurity readiness and requirements and reporting measures. But, these attacks that I just referenced highlight the interconnectedness of the healthcare ecosystem. And, in fact, over 95% of the attacks on the healthcare sector came through the third parties. And, why is this happening? As was mentioned previously, we're seeing a rise in a lot of the nation-state actors who have realized that, as hospitals and other

facilities have actually built up their safeguards, they would prefer to do a hub-and-spoke model, which is, "Hey, let's attack this third-party vendor that has access to all this other data, and if we attack them through this one entity, we have the access to a bunch of different other facilities and healthcare systems." So, as hospitals and other facilities are building that up, the vulnerabilities are really in these third parties.

So, what have *we* been doing as hospitals over the last few decades, to be honest? As I mentioned, we comply with Federal standards; with HIPAA requirements or other requirements within the Health and Human Services Department, within the Federal government. We do all these risk assessments, exercises, etc. We purchase cybersecurity insurance, which is quite costly, but necessary. However, hospitals' efforts alone cannot address the full scope of these threats. To strengthen the healthcare sector's cybersecurity posture, NJHA recommends a few of the following items for your consideration:

1. Going back to third parties is enhancing the oversight of these third parties. There is a secure-by-design, secure-by-default process put out that's widely accepted by the hospital community we think should have application to these third-party entities, making sure they have the same cybersecurity standards that we have, since they are, in essence, accessing and handling all of that sensitive patient-level information.

Streamlined financial support during an attack. So, what happened during Change Healthcare, it took a few weeks, but eventually Medicare provided advanced payments to hospitals to deal with the revenue flow. These weren't-- This wasn't free money; this was money that was paid in advance and then reconciled at the end of the month to make sure that

the payments matched up with the care that was delivered. But, a consideration is requiring insurance companies to provide these advanced payments to help hospitals maintain the financial support during an attack.

Regulatory alignment. Making sure, as Chris mentioned, when we have kind of different sources of reporting in and you have the Feds regulating in the state just having some alignment and some streamlined reporting requirements on hospitals.

And, then, the last I'll mention is support for nonprofit providers in regards to cybersecurity insurance. So, as these threats become bigger and bigger and larger and larger, the price for cybersecurity insurance has significantly increased. So, some acknowledgment for -- especially nonprofits that *have* to purchase cyberinsurance -- having some sort of safeguards and requirements on these insurance companies that the rates don't go through the roof.

So, I will pause here. I am happy-- I appreciate the opportunity to speak today, and I'll take any questions or comments.

Thank you.

SENATOR GREENSTEIN: Thank you very much.

Do we have a-- Yes, Senator.

SENATOR McKNIGHT: Yes, I have a question.

Neil, so, with these attacks-- You spoke about the employees; you spoke about what you do in-house.

What are some things that you do in reference to the patients? Where, this is their information.

MR. EICHER: Yes. And, quite frankly, that's the fear, is that patient-level information will get out there. Specifically sensitive information.

There are requirements that when a certain number of patient medical records are exposed, the hospital has to notify those patients about the exposure. There are requirements, and hospitals notify the FBI. They work with NJCCIC; they work with the Feds, to make sure, hey, this happened, let's get this information out and let's figure out what to do and do a threat assessment.

But, you're absolutely right. Is this very vulnerable information out there that could potentially be exposed if hackers get in?

SENATOR McKNIGHT: So, is there anything that you recommend that the Legislature can do to help you help the patients? Because some of their information is very vulnerable.

MR. EICHER: Yes, I would go back to the third-party point that I -- the third-party entity point.

Because, as hospitals are required to share patient information with the State Government, with Federal Government, how do we ensure that everything along that pathway is fully safeguarded that information? So, the hospital may be doing everything it can to protect it; how do we ensure that these companies are actually doing it, too? So, whatever increased safeguards we can put on those would help the hospital industry and protecting the patient information.

SENATOR McKNIGHT: Thanks.

And, Chris, the same question in reference to customers. So, what are some things that the business industry is doing if there's an attack, and now there's customer information that's out there?

MR. EMIGHOLZ: There are-- As Neil said, there are similar requirements.

I think all of us have probably gotten a -- been on the receiving end of a letter that we got from one of our providers, insurance companies, businesses, whatever, you name it, that there's been some leak and they don't know what's out there. And, I think that businesses comply with those rules. A lot of those rules are from Federal Government, as I think that's probably where the place should be.

But, I think, is there more that the State could do to -- I think, looking into supporting -- I mean, I think patients, customers, on, you get -- the State can support credit check for somebody who was on the receiving end of cybersecurity incidents, and could the State do things like that? I think that would be welcome, I think the State could do things, support, but it probably gets tricky for the State to add new enforcement, because I think we have a lot of those things already.

SENATOR McKNIGHT: So, last point.

I will say, those letters -- because I've received some of those letters. And, they're very-- There's too many words. And, sometimes, I think it's junk mail.

So, I will recommend that there's something that we do different with these letters that's coming to customers and patients when there is -- when their information was exposed. Because, I look at them like, "OK, what is this?" It's just too much. And, it's not -- it's not -- it's not -- I don't read

it as being sympathy or empathy, it's just like, "Hey, this is what happened, and call this number, and that's that."

So, I'm just putting that out there.

MR. EMIGHOLZ: Good feedback, and I will take that back to our members.

SENATOR McKNIGHT: Thanks.

MR. EMIGHOLZ: Thank you.

SENATOR GREENSTEIN: I think the Senator makes a good point. Not only-- These days, it's very hard to tell if something is a scam. And, I know I had-- Once I was a victim of a scam, which I never thought I would be, but I was. And, it's very hard to tell.

So, some of the letters that may be coming to help you, you can't always tell if they're real. My first thought is always that they're *not* real, so it becomes a problem.

OK, thank you both very much.

MR. EMIGHOLZ: Thank you.

Happy holidays.

SENATOR GREENSTEIN: Thank you.

Next, we'll have Hilary Chebra -- South Jersey Chamber of Commerce; and Tigran Safari -- CISO Global, representing New Jersey Bankers Association.

Why don't -- we'll start with Hilary.

H I L A R Y C H E B R A: Thank you, Chairwoman.

Good afternoon, members of the Committee.

Hilary Chebra; I am the Manager of Government Affairs for the Chamber of Commerce Southern New Jersey.

Thank you for the invitation to come and testify today.

I am going to talk a little bit about what our members are doing to protect against cybersecurity threats, and then provide some recommendations of how our partners in the Legislature can be helpful to our members.

Just a little bit about our Chamber: We have approximately 1,200 members, 85% of which are small businesses that employ less than 50 employees. And, I bring that up because small businesses, as we've heard, are often disproportionately affected by cybersecurity attacks. They often have less resources to provide an in-house IT department. They also are much less likely to be able to have the resources to recover after a cybersecurity attack. So, again, I bring that all up to say most of our membership is small businesses, and that's a lot of what we're seeing as the target for the cybersecurity attacks.

So, what are businesses doing? A lot of folks are investing in the infrastructure that we've heard a little bit about: Next generation firewalls; end-point protection; network monitoring, to help mitigate these threats in real time; and, regular software updates -- a lot of things that we've already heard a lot about. And, something we've heard repeatedly is noting that a lot of cybersecurity entry point is through human error. A lot of increase on employee education and programs to help train them to mitigate these threats. So, like I mentioned, small and mid-size businesses are going to partner with managed security service providers to oversee threat protection.

So, what can the Legislature do and partner with the business community to help protect our businesses? We would recommend State-funded cybersecurity grants and tax incentives. As I've mentioned, small

businesses are often the ones who are going to bear the brunt of these cybersecurity attacks, so anything we can do to help these small businesses; these mom-and-pop shops; these small third-party vendors, that work with the big businesses, that could be an entry point to the cybersecurity attacks if we can provide some sort of funding. Tax incentives, grants can really go a long way to helping them bolster their protection.

And, as Chris mentioned, we agree that promoting public-private partnerships in cybersecurity training and workforce development is key to continuing to be able to combat these attacks. And, this is an ever-evolving threat, as we've heard, that things are getting more sophisticated, and if we have a workforce here in New Jersey trained to address and be able to learn along with what is going on currently, then we can have a better chance to mitigate the cyber risks moving forward.

So, those are some of the things that our businesses are doing; those are some of the things that we think will go a long way in helping our businesses, both large and small, in combating these cyberattacks.

SENATOR GREENSTEIN: Thank you.

Are you Tigran?

B R I T T A N Y W H E E L E R: Good morning, Chairwoman.

No, I am Brittany Wheeler, with New Jersey Bankers Association. And, I just briefly wanted to introduce myself.

And, our Association represents 66 brick-and-mortar institutions from systematically important institutions down to single-branch entities. And, we have roughly 200 associate members as part of our team. Out of the 66 brick-and-mortar institutions, roughly 40 are State-chartered institutions, regulated by the New Jersey Department of Banking and Insurance.

And, I would like to acknowledge that cybersecurity is an ever-evolving threat and challenge, and it is critical that our financial institutions, along with government partners, remain vigilant and proactive in addressing emergent threats. And, in preparation for today's testimony, I spoke with several individuals who sit on our New Jersey Banker Cyber Risk Committee. And, one common theme that I wanted to highlight is that our members -- in this space in particular -- view themselves as colleagues, not competitors. And, that has helped to really foster a culture of vigilance when it comes to this matter across our state, and it's something that we're very proud of.

And, now, I'd like to turn it over to Tigran Safari, who is our subject-matter expert on this issue. And, Tigran is the Chief Information Security Advisor for CISO Global.

So, I'll turn it over to him now to answer your questions and provide testimony.

TIGRAN SAFARI: Madam Chairwoman, members of the Committee, thank you for the opportunity to testify before this esteemed Committee on the critical subject of cybersecurity in the banking sector.

My name is Tigran Safari, and I have decades of practical experience managing cybersecurity challenges for financial institutions, and advising our strategists to safeguard customer data. As they trust the Chief Information Security Officer with CISO Global, I work with banks; credit unions; and other businesses in the energy, insurance, and healthcare sectors, ensuring that the infrastructure remains resilient against evolving cyberthreats.

Banks' proactive and Federally mandated investments in cybersecurity have set benchmarks for resilience and innovation. These

investments showcase the financial sector's leadership in safeguarding data, even while remaining a key target for bad actors. Financial institutions are looking at an average of 10-12% of their IT budget to cybersecurity. Double that of other sectors, showcasing their leadership in the space. The banking sector employs a comprehensive multi-layer cybersecurity strategy known as "defense depth" to address these growing challenges. This fail-safe approach ensures that even if one layer of defense is threatened, others remain operational to mitigate risks and protect sensitive assets.

But, even with the state-of-the-art systems, spotting real cyber incidents can be tricky. Monitoring tools generate countless alerts and false positives, making human-added touch crucial to identifying real threats. Mandatory reporting requirements often distort comparison with other industries. In 2023, statistic reports highlighted that banks reported more cyber incidents than other sectors. This reflects their transparency and proactive approach -- not greater vulnerability. Many banks rely on third-party service providers, or service bureaus, to manage operations and handle large amounts of data. This dependence poses specific risks -- interconnected risks, accountability, and fourth-party dependencies.

However, Federal regulations and strong partnerships between banks and these digital warehouses effectively mitigate these risks. Unlike service bureaus, managed security service providers -- MSSPs -- focus primarily on cybersecurity. Federal agencies recognize them as critical vendors, and require MSSPs to provide evidence verifying their qualifications to deliver cybersecurity services. Banks and Federal examiners thoroughly review MSSPs' due diligence packages to ensure compliance and reliability.

To summarize, through a Federal verification, MSSPs enhance banks' existing cyber efforts, providing the expertise to identify cyber incidents, and the solutions needed to respond effectively when incidents occur. This partnership ensures financial institutions remain resilient, prepared, compliant, and ready to act -- even in a dynamic threat environment.

In conclusion, cybersecurity in the banking sector exemplifies a continuous dynamic commitment to protecting customer data in public trust. The banking sector is the only industry with a unique 36-hour incident reporting requirement mandated by Federal regulations. This ensures swift action, and reinforces public trust by setting a higher standard of accountability. This requirement underscores the sector's exceptional commitment to transparency and speedy action. It also reflects the high level of cyber maturity in the financial industry, where advanced systems and processes are in place to identify and report incidents efficiently, ensuring both public and private data remains secure.

Thank you for allowing me to share these insights.

As we move forward, I encourage this Committee to recognize the banking sector's exceptional efforts and unique challenges in cybersecurity.

I am ready to address your questions.

SENATOR GREENSTEIN: Thank you.

Do either of you have questions? Either one? (no response)

OK, I guess we don't have any now, but that doesn't mean we won't be calling, because this is great stuff that we've been hearing, and I'm

thinking to myself I'm going to want to call various people who we've heard from today and get more information.

So, thank you very much. I really appreciate it.

MR. SAFARI: Thank you.

SENATOR GREENSTEIN: We have just two more people, and then the hearing will be over.

We have John Indyk -- Healthcare Association of New Jersey; and, Ed--

E D W A R D R I Z G A L L A H: RIZZ-GAL-UH.

SENATOR GREENSTEIN: RIN-GAL-UH? RE-GAL-UH?

CEO at Christian Health.

Thank you.

J O H N I N D Y K: Madam Chair, thank you very much for this opportunity.

Thank you for the invitation to appear before you.

I am certainly no expert on this, but I do know it touches everybody's lives on the home front. Our trade association-- I am John Indyk with the Healthcare Association of New Jersey. We represent over 300 nursing and assisted living facilities. Not all providers-- There are other threats by other entities. We have the bulk of the long-term care sector. Our trade association was subject to a cyberattack one day -- I believe it was when we were at a conference, so it shut down our computer system. Luckily, we caught it in time; we had an IT professional consultant who advised us on how to protect our data. So, because we have "healthcare" in our name, I don't know if it's because we're a healthcare entity and they think we've got

something that they're after, or they wanted to be a conduit to conduct nefarious activities elsewhere.

But, I do know our members, since 1996, we have the Health Information Affordability and Accountability Act to protect the data of people receiving healthcare. So, we have long been dealing with that, on that perspective. But, cybersecurity has a different feel to it, so-- And, I agree with many of the recommendations that Neil talked about, particularly third-party entities like Change Healthcare. When they were cyberattacked, it drastically disrupted the cashflow into our communities. And, I would strongly encourage you to look at that, because that's who they're going after. And, the cashflow to us -- we operate on very thin margins, and it gets very disruptive, especially for the small mom-and-pop facilities. It's-- I would encourage you to look at that.

Our facilities do incur administrative costs. Ed, who I am here to introduce, really, can speak more to what he does, but there was a time when you didn't have to worry about this. So, it's an added expense that takes away from direct-care patients. So, we are constantly getting new things that we have to expend money on that don't relate directly to healthcare delivery, but they do protect the data and sensitive information of our patients.

So, I will turn it over to Ed, and he can go more into detail on exactly what our facilities do.

SENATOR GREENSTEIN: Thank you.

MR. RIZGALLAH: Thank you for the introduction, John.

Thank you, Senators, and Committee members.

My name is Edward Rizgallah; I am the Chief Information Officer at Christian Health in Wyckoff, New Jersey. I have about 25 years of healthcare IT experience.

I would like to share from my experience some insights and maybe some best practices that, from what I'm seeing in the industry, maybe a lot of people are not taking advantage of like they should.

Number 1. Cyberinsurance. We've talked-- We touched on cyberinsurance briefly, but I don't think a lot of businesses take full advantage and get their money's worth from cyberinsurance. So, for instance, many may not know that your cyberinsurance agency has a 24/7 command center. And, they should really be your first point of contact. They have a wealth of resources from forensics to legal advisors. They actually offer you a legal team in case there is a breach. And, they will reach out to the authorities if that's something that they deem necessary.

It also is in their best interest, as your insured, to make sure that you're secure. So, they'll offer to help with policies and procedures. They'll also assist with your emergency-response plans, and they'll also execute tabletop exercises with you. So, they'll do mock incidents to walk you through what it would look like in the event of a breach. So, that was the first item.

And, speaking of emergency-response plans and outages, it's important to have all your documentation in place. And, I think a very common oversight is people will store their emergency-response plans somewhere that's affected by the outage itself. So, in the event of an outage, they no longer have access to it. So, one of the things that I recommend is make sure that you store all your documentation -- your policies and

procedures, your emergency-response plan -- somewhere that's accessible in the event of a global outage.

Cloud services is something that sounds very fundamental. This day and age, I would imagine everybody is taking advantage of all their applications and systems is offered as software as a service. So, in most organizations, I would imagine this point in time your IT closets don't necessarily have a lot of servers in them; they have mostly telecom equipment -- switches and routers and things like that. Minimizing the amount of physical hardware you have on prem reduces the liability. So, when you engage with a partner that offers to house that information, there's a shared liability; there's contractual BAA agreements and things like that that offset some of the liability that you might experience during an outage or a breach.

Multi-factor authentication -- we heard about that earlier. It sounds very fundamental, but a lot of businesses are taking advantage of it from the extent where they're using Office 365 and they're requiring their end-users to have multi-factor authentication just to get into Windows. Really, all your applications should have multi-factor authentication. So, if your billing system should be on it; your electronical medical record; anything that stores sensitive information should leverage multi-factor authentication.

Phishing -- Michael spoke about phishing; and I agree with everything he said about phishing. It is the least point of resistance for a cybercriminal. You're not going to see cybercriminals these days -- often -- try to penetrate a firewall unless your firewall is poorly configured, or you've left ports open on your firewall. That's not going to be a common occurrence. If you're going to get hit, most likely it's going to be through an email. Nine out of 10 times, or 99 out of 100 times, it's going to be through an email.

So, that's where we put a lot of our emphasis. So, we see how relentless these attacks are getting through email. Pretending to be our CEO; pretending to be our Chief Financial Officer asking us to wire money. And, a lot of these end-users are falling for it. So, we are very aggressive with running phishing campaigns and training exercises. We run multi-campaigns a week, and we identify repeat offenders, and we make sure those repeat offenders are trained and held accountable. We even established an HR policy, that if you become victim to a phishing email a certain amount of times, there's a corrective action that needs to be taken.

And, lastly, I wanted to just bring up, again, it was mentioned before -- Chairman. So, a lot of people take procurement very lightly. What I'm seeing is that they trust these third-party vendors with their standardized contracts, their standardized BAA agreements, and they just sign off on them, taking them very lightly. There needs to be a lot of scrutiny on these contracts and these agreements, because often times these third-parties -- these vendors -- need your data to provide the service that they're giving you. And, so, now, what you've done is you've handed off all your data to a third-party, and you've multiplied your liability. And, you need to scrutinize and red line the hell out of these contracts to make sure that you're properly protected.

And, with that, I will open up for questions.

SENATOR GREENSTEIN: Thank you.

Question?

SENATOR MORIARTY: I definitely agree with you on the phishing; that's where people are going to get to you. And, I think that I like

what you had to say about people repeatedly fall prey to these, that this corrective action -- I think we should be doing that in our State as well.

Because, if someone is going to keep doing the same bad thing and exposing the healthcare operation of the State to bad actors, it's no different than a security guard who is supposed to be guarding that door and they're asleep. So, there *has* to be repercussions, and we need to do that, I think, as a State.

I wanted to ask you about insurance, because of course the insurance company has a desire that you're protected; otherwise, they're going to have to pay a ransom. Now, I don't know what their liability is, because you buy insurance, you're going to buy insurance for $100,000, $50,000 -- whatever the -- you decide on. And, the premium will reflect what you decided on.

But, how does-- How do businesses understand which is a good company?

MR. RIZAGALLAH: That's a very good question.

SENATOR MORIARTY: I mean, you've got to worry that someone who is offering you cyberinsurance may be the wolf himself, right?

MR. RIZGALLAH: Yes, absolutely. Absolutely.

And, my recommendation to that -- so, not only do we have our cyberinsurance organization, we also have a HIPAA attorney who works independently. So, we take everything they say with a grain of salt, because we understand that they don't want to reimburse you a $10 million in damages of a ransomware breach.

So, we consult with our HIPAA attorney, and she gives us legal guidance in that matter. But, you're absolutely right. You have to tread carefully.

SENATOR MORIARTY: Are there any industry guidelines that you know of, that rates cyberinsurance companies?

MR. RIZGALLAH: That's a tough one. I mean, we use an organization called Beazley. I know they're very reputable in the industry, and healthcare specifically. But, I don't now the answer to that. Maybe somebody like Michael would have some recommendations or guidelines.

SENATOR MORIARTY: Sure.

Thank you; thank you very much.

MR. RIZAGALLAH: Yes, absolutely.

SENATOR GREENSTEIN: Yes.

SENATOR McKNIGHT: So, my question to you is, companies get the McAfee, (indiscernible) for software -- for security software.

What are some other things that companies should have in place on their computer to help mitigate and comb through attacks?

MR. RIZGALLAH: Yes, so, I can't emphasize the email enough. Email is the biggest risk. So, I think it should be pretty standard; you should have some kind of quarantining software in your inbox that uses algorithms, it uses AI, to identify what could potentially be a phishing email, or some kind of malicious threat, and it filters it out for you.

SENATOR McKNIGHT: So, now, do you have a list of recommended -- recommendations of companies to use? Because, just like the Senator just mentioned--

MR. RIZGALLAH: I can probably come up--

SENATOR McKNIGHT: --one of them can be a wolf.

MR. RIZGALLAH: Absolutely. I could probably come up with a list; I don't know if I could rattle a bunch off the top of my head. But, yes, I know what we use.

SENATOR McKNIGHT: That would be great if you could send it to the Chairwoman--

MR. RIZGALLAH: Absolutely--

SENATOR McKNIGHT: --to send out. That would be great.

MR. RIZGALLAH: I would be happy to.

SENATOR McKNIGHT: Thank you.

SENATOR GREENSTEIN: OK.

Well, thank you both very much--

MR. RIZGALLAH: My pleasure--

SENATOR GREENSTEIN: --really appreciate it.

And, meeting adjourned.

(MEETING CONCLUDED)