As a New Year Begins, Threat Landscape Takes a New Shape

CYBERSECURITY: AI Thrown Into the Mix; Need for Cyber Professionals Remains High

■ BY BRAD GRAVES

If past is prologue, cybersecurity issues are sure to grab headlines in 2023.

The way businesses approach that threat, however, is still within their power.

With that in mind, the **San Diego Business Journal** and the **Cyber Center of Excellence** (CCOE) produced the first installment of the 2023 Cybersecurity Trends series.

As usual, the discussion was moderated by **Lisa Easterly**, president and CEO of CCOE. The San Diego-based nonprofit mobilizes businesses, academia and government to grow the regional cyber economy and create a more secure digital community for all.

"Cybersecurity is now everyone's business," Easterly said, "with the **FBI** reporting a 300% increase in cyber crimes across all industries since the pandemic began." The average cost of a data breach has climbed to more than $4 million, she said. "Unfortunately, more than half of these costly attacks are aimed at small and medium-sized businesses, which are our region's economic engine.

"Now pair that with the global shortage of cyber professionals to thwart these attacks—to the tune of about 755,000 openings in the U.S. and about 81,000 here in California—and it becomes mission critical to address the workforce gap.

"The good news is here in San Diego, we're leading the charge with more than 870 cyber firms and the **U.S. Navy**'s **Naval Information Warfare Systems Command**. The cluster now accounts for more than 24,000 jobs and has a total economic impact of $3.5 billion annually, and that's equal to hosting nine Super Bowls. This collaborative ecosystem is developing new technologies, defenses and cyber warriors to combat these ever-evolving threats."

With that, Easterly introduced the panel and the topics, namely what San Diego businesses and workers need to know about the current threat landscape, as well as workforce trends.

Eric Basu, founder and CEO of **Haiku**, introduced himself first. "We create videogames that actually teach cybersecurity skills. And by doing this, we've found we've actually been able to increase both the diversity and the opportunity for people to be able to get into cybersecurity by making it far more accessible to them.

"In a previous life, I was an officer on the SEAL teams and I ran a company called **Sentek Global** that was a defense contractor in San Diego."

Richard Portelance introduced himself next. His company, **Journeys Map**, started about eight years ago in San Diego. "Our mission is to bring people into the world of cybersecurity by matching where they are currently to the possibilities of a career change," he said.

"We work with students from K through 12 all the way up through career transitioning adults and workforce participants to help them figure out new careers. Our mapping solution has a robust underlying dataset that includes everything from state education standards, CTE standards. We also have a robust repository from **College Board** and a job index from **Indeed** as well as many other data sources that we brought together in one place for a visual map for people to be able to take the steps from where they are today to where they want to go. And we built a cyber specific mobile application. We're happy to offer that through CCOE as well."

Cybersecurity veteran **Miguel Sampo** introduced himself next. "I'm dating myself now in the cyber industry; I think I started in this before there was even a cybersecurity practice.

"I'm part of **RiskRecon**, which is a **MasterCard** company," Sampo said. "We specialize in third party risk management. One more layer of security in that Security in Layers phenomenon that we see protecting organizations. What I find most exciting is just the evolving threat landscape, the sophistication of the technologies that we have to use, and also, not to give credit to the bad guys, but the sophistication of the attacks that we're seeing. So it's been a lot of fun, working with all different verticals, working with our community here as well, and so excited to be here and be part of the panel today."

Insurance Landscape Changes

At that point, Easterly started the conversation: "We're going to kick off our discussion with the trends we're already seeing take shape this year, from ransomware as a service to AI-driven social engineering to major changes in the cyber insurance market."

Turning first to **Eric Basu**, she asked about key threats that all businesses should have on the radar this year.

➡ *Cybersecurity page 44*

MODERATOR

LISA EASTERLY

Lisa Easterly serves as president and CEO of Cyber Center of Excellence (CCOE), a San Diego-based nonprofit that mobilizes businesses, academia and government to grow the regional cyber economy and create a more secure digital community for all. Prior to joining CCOE, she was the Vice President of Marketing for San Diego Regional EDC, Business Development Manager for Latham & Watkins LLP and Founding Board Member of CleanTech San Diego. She has an MBA and B.S. in Finance and Economics from the University of Florida.

THE PANELISTS

ERIC BASU

Eric Basu is the founder and CEO of Haiku Inc., a maker of videogames and gamified training simulations for those wanting to learn cybersecurity skills. Previously Basu founded, built and sold Sentek Global, which grew to be the largest small defense contractor in San Diego. Basu has an MBA from the EMBA program at UCLA, a B.S. in Molecular Biology from San Jose State University, and is a former U.S. Navy SEAL officer.

RICHARD PORTELANCE

Richard Portelance is General Manager for Journeys Map. With a deep desire to help people succeed, Portelance has led teams and projects in digital marketing, edtech and cybersecurity during a career that has spanned three continents over the course of three decades. Having worked with many passionate professionals, he is committed to helping every learner fulfill their potential and find success.

MIGUEL SAMPO

Miguel Sampo is Senior Director with RiskRecon, a MasterCard Company. He has more than 20 years of professional cybersecurity experience working with Fortune 100-1000 organizations. He is a strategic thinker with strong technical skills mirrored with the capability for problem solving and building solutions. He has proven experience on every side of "the business" from sales, sales engineering, product management, to business development, which has provided him with broad business and technology industry acumen. He is a member of the Cyber Center of Excellence (CCOE) board.

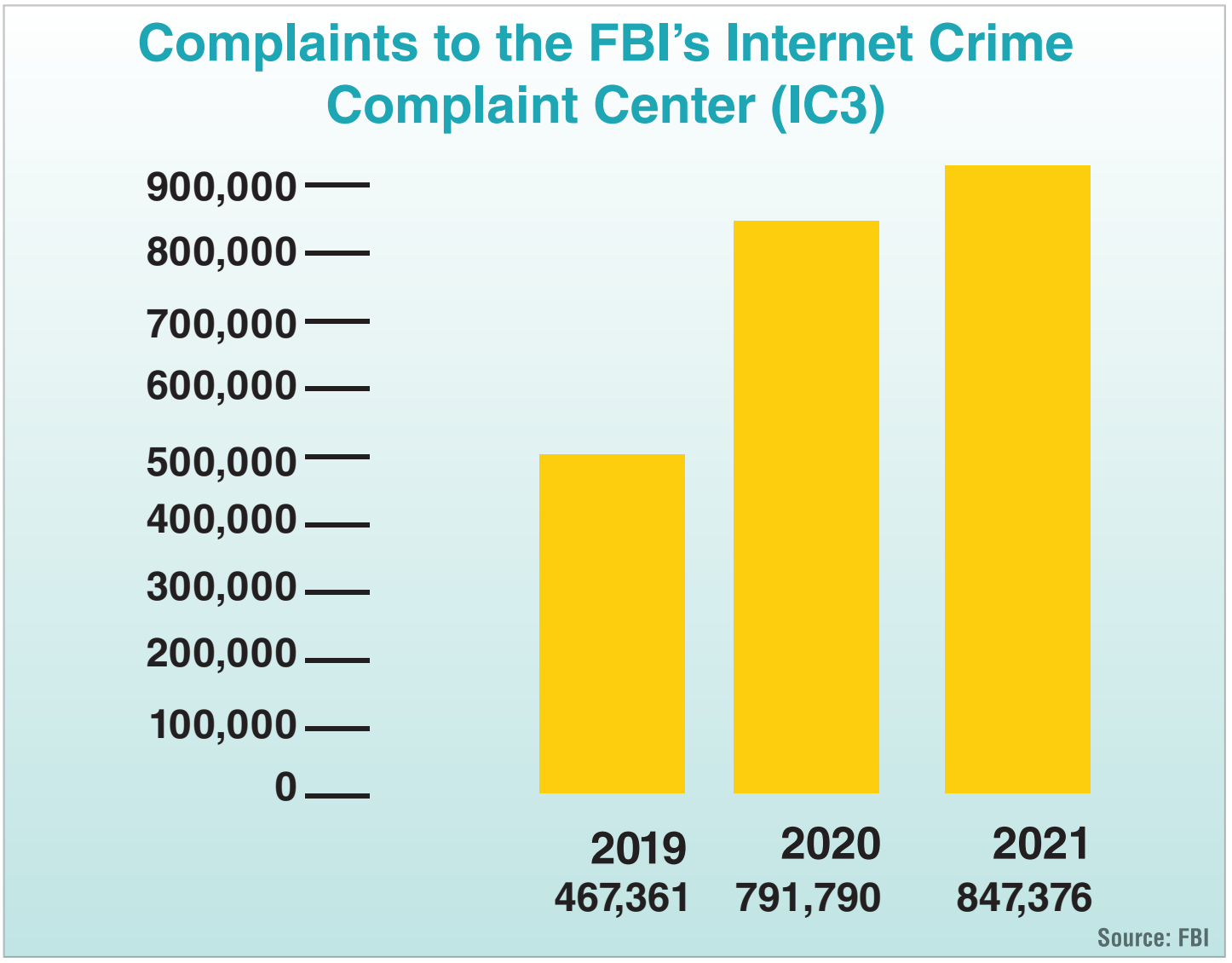
Cybersecurity

➡ *from page 42*

"What's really interesting is there was a recent article about **Merck**," Basu said. "They were hit by a cyberattack and their insurer refused to cover it because they said it was a warlike act. That's a huge sea change in how businesses are going to react because they have always come at the problem from the following perspective; for a while there, they didn't have any insurance at all until the **Target** CEO got fired [following a data breach]. He was the first major company CEO to get fired for that. Then, they all bought insurance and thought, 'I'm good. I pushed the insurance button.' Now they're looking at it going, even if I buy insurance, my insurance might not cover it, which might lead again back to the executive team getting fired.

"I think that's something that, if I were a CEO of a large company—and I'm a CEO of a small company—I would be looking at very carefully and saying, 'What are we doing with our insurance? And will my insurance cover an act of war or will they call it warlike?' That will be litigated as well.

"One of the other things I think people need to look at is that we have a lot of warfare going on. Russia invaded Ukraine. And so we're going to see a lot of nation-state type of actions that are coming as countries step in to help Ukraine. They may end up being targeted by Russian cyber attackers."



Hackers Benefit from New Tech

Basu then turned to technology trends, including those involving multifactor authentication, or MFA.

"I've been hearing some things about MFA attacks, being able to defeat MFA. You know, MFA has become a lot more popular, a lot more common, thankfully, so now you're seeing hackers starting to focus on how do they get rid of MFA, how do they do a SIM cloning so that they can actually intercept the text that comes to your phone? And you're going to see people shifting their MFA type of responses based upon that.

"Another interesting one is the use of ChatGPT, the **OpenAI** product that's come out. I saw a great meme on this saying, OK, we all found that ChatGPT AI can now be used during attacks. So if you work around ChatGPT—and they try to improve it all the time—you could actually get it to build malware that could get an iPhone. It's the same sort of thing that we had when basically the most sophisticated attackers, ones that had personal skills, then you had script kiddies that could download things. And suddenly that opened up the attack surface.

"So I think ChatGPT has taken it to another level. And not just them; I don't want to pick on them. Any AI [can do it] because they're basically enabling other people to be able to write malware, in this particular example, that could basically compromise an iPhone. And so I think that's probably something that needs to be looked at as one additional threat, and certainly something you can't ignore. I'm going to have more people trying to attack my company."

"I know, I keep saying I've seen this movie and it doesn't end well for humans," Easterly joked. "One of the big trends we saw last year and I think continues into this year is that considerable uptick in supply chain attacks as cyber criminals attempt to fracture the backbone of our global production in critical sectors like food, energy, manufacturing and so on," she said.

Recognizing Vectors and Other Best Practices

Easterly then turned to **Miguel Sampo** and asked about best practices and resources for small to medium-sized businesses "that are often the entry point and unfortunate casualties of these supply chain cyberattacks."

"There certainly was an uptick in what we saw," he said. "And to back up for a second to Eric's point, we talked about cyber insurance and we see that being weaved into supply chain and organizations that are seeking to get a policy for cyber insurance, making sure that not only are they protected within their own environment, but how much inherent risk have they introduced by doing business with their supply chain? Or third parties and fourth parties?

"Having a good idea of what that inherent risk is, is becoming critical," Sampo said. "And insurance companies are starting to use tools that will give assessments or cyber rating scores on not only their own organization, but also the supply chain or their vendor landscape. I don't have a crystal ball, but I would predict that over the course of the next 18 to 36 months, we're going to see something like that. And probably so, we'll see some kind of standardization on some kind of a scoring methodology. Today in the fintech or financial world, we have a standardization score like FICO. Everybody's pretty familiar with FICO. And so we're going to see something very similar coming in cyber.

"Going back to the supply chain attacks and the things that we've seen, Lisa, I think one of the most important things that we saw is that nobody's immune," he said. "There isn't a vertical [market] that is safe. All verticals are targets for the bad guys: healthcare, manufacturing, food, you name it. Retail technology. All of them, they've all been victims to some degree. And the key theme that we see is educating our users.

"And so my first best practice that I would recommend is recognizing what the vectors are. What are the vectors that these bad guys are using? And I'm not going to go into a lot of detail for the sake of time, but I will name a couple of these.

"Email. We use email every day. Understanding how to safely use email, not falling victim to phishing or vishing attacks. Running enablement sessions so that our users understand email security is an area of focus that I would recommend for organizations, whether you're a small shop, a medium-sized shop, or a large shop. I know it sounds kind of hokey, but know how to use email safely.

"The other component that we see is that there's a lot of organizations that are building applications or using applications. Eric talked about script kiddies and stuff. Building applications has become so much easier nowadays. There are tools that will automate that process and build those for you. The problem with that is, though, you build applications that haven't been vetted by a security practitioner, you put it out on the web and you make it publicly available, now you're subject to an exploitation or numerous amounts of vulnerabilities. So properly vetting applications that you're using, buying and building is critical.

"The other component that I would say is vulnerabilities. Everybody has to have some responsibility around patch management. Understanding that your systems are up to date and running safe systems is one of the key 1-2-3's or the 101's of making sure that you're doing safe computing.

"There are a lot of other vectors that we can get into. Working closely with your InfoSec teams, if you have one. Anything that's publicly facing, understanding what that looks like and what's the threat or the potential vulnerability.

"Part two, kind of the best practice approach is—I'll say it and you hear me say it all the time, Lisa—Security in Layers. The days of antivirus and a firewall are not sufficient anymore. I mean, we have got to use things beyond that. And so one of the things I recommend is that when you look at your tool sets, having tools that provide automation, whether it's an automated assessment, automated scans, things of that nature are going to be fundamental to your cyber program. Continuous monitoring solutions need to be more prevalent.

"And then physical. Running tabletop exercises in the event of a breach. How do we respond? What is step one? What is step two? Having a plan, I think, is part of that.

"And then the last component is working closely with your partners and your reseller community, whether it be your MSP or somebody that manages your SOC [security operations center]. If you do outsourcing, working with them and understanding what safe practices they bring, how do they invoke that and having a contingency plan. Those are the best practices that I would recommend.

"Locally, I definitely want to make a sound bite that the CCOE has been working to increase cybersecurity awareness with several of the

➡ *Cybersecurity page 46*

CAUGHT IN THE CYBERSECURITY TALENT SHORTFALL?

There are over 600,000 open cyber jobs, and the FBI reported a 300% increase in cyber-crimes during the pandemic. Is your business keeping up?

San Diego businesses and non-profits are turning to **Journeys Map** to create robust, automated cybersecurity talent pipelines. A bridge between learners, workers and businesses, **Journeys Map** leverages patented technology in the creation of accurate and trackable career maps that take participants from where they are today, to where they want to go.

What you get from Journeys Map:

NIST Framework

Integrated state & federal educational standards, and the NIST/NICE framework

Custom mapping & assessment options to suit your business needs

Robust tracking and reporting features

Integrated Cyber specific work-based resources like podcasts, events, and articles

San Diego CCoE

Integrated with CCOE cyber job board and Indeed™

To learn how your business can build a robust cybersecurity talent pipeline, contact **Journeys Map** today.
hi@journeysmap.com

Journeys

CAREER JOURNEYS BEGIN HERE

San Diego Business Journal Special Offer

Click to get **10%** off program setup and subscription fees: www.journeysmap.com/sdbj

Cybersecurity

➡ *from page 44*

local municipalities and offering cyber awareness and preparedness programs for small businesses. We have teamed up with the CCOE and we, **RiskRecon MasterCard**, offer free trials on our website where you can run a scan and scan some of your vendors as well. But even more importantly, the CCOE also offers free assessments, free scans [for those] that are part of the program. I know city of Carlsbad, city of Vista, city of San Diego, and several others that are hosting the program. So we're excited to be able to offer those in our community as well."

"It's been so much fun to be able to partner with organizations like **MasterCard** and **ESET** and **CyberCatch**, the **FBI** and many others to provide small businesses with awareness and preparedness so that they have a better concept of the threat landscape and their own cyber posture," Easterly said.

Getting Connected

"So I think, as Miguel and Eric alluded to, creating a culture of cybersecurity is really mission critical for organizations now," said Easterly, turning her attention to **Richard Portelance**. "Rich, how can resource-constrained small to medium-sized businesses effectively educate and mobilize their employees and business partners to become stewards of cybersecurity, hygiene and awareness?"

"That's a great question," Portelance said, "and I think it's on everybody's mind. How do we get more thought leadership within that space? Small businesses, as you pointed out at the beginning, Lisa, are under attack, more so today than ever before. And I think the number one thing people can do is take advantage of the opportunities that are at hand, like a CCOE. Not to be too indulgent in promoting what you do, but it's really essential for small businesses. I mean, here we are, our people that are in the San Diego area, and we are taking advantage of the fact that there is an aggregate group of likeminded individuals who bring about opportunity to become aware, become trained, whether it's through a Haiku or other kind of solution, the small to medium-sized businesses and other businesses need to look into that community. So some of the things that CCOE has done, and I think it's really powerful, is bringing about some of the education leaders within the sector so that these businesses can find talent and bring them in, in order to become more aware of what the cybersecurity threats are, how to better protect themselves. And if they can't hire those individuals themselves, they can bring in the right resources in order to protect their business. So it's a constantly evolving landscape. So I would definitely say, look outside of your own company and take advantage of what's out there. Get connected to the schools and industry professionals that are in the community.

"One of the things that we're doing too is bringing about opportunities for the younger professionals and the students. One of the cool things about cybersecurity is you don't necessarily have to have a college degree in order to become a cybersecurity professional. And so the more we interact with the local high schools, the more opportunities we can give those young people to see those career opportunities and present them, and then find the path to get a cybersecurity job within a year after high school, or two years after high school. They can get the proper training to start off at the bottom level and work their way up. And what we're finding from these younger professionals is they bring some real world experience. They understand the mindset better than some of us older people do, just because they're living it, they're in that world on a daily basis and they understand what's happening. So we definitely take advantage of the fact that there are programs, there are a lot of schools in the region that offer cybersecurity programs. And then there are really unique companies like Haiku and others that are offering programs that will train professionals very quickly to at least have a baseline understanding of how to take advantage and protect the company assets from cyber threats."

"Well, I think you hit the nail on the head," Easterly said. "The shortage of cybersecurity professionals continues to be a challenge across all industries, including more than 10,000 openings here in the San Diego region. Miguel, can you talk a little bit about how employers can evolve those job reqs to cast a bit of a wider net and what criteria you recommend they focus on?"

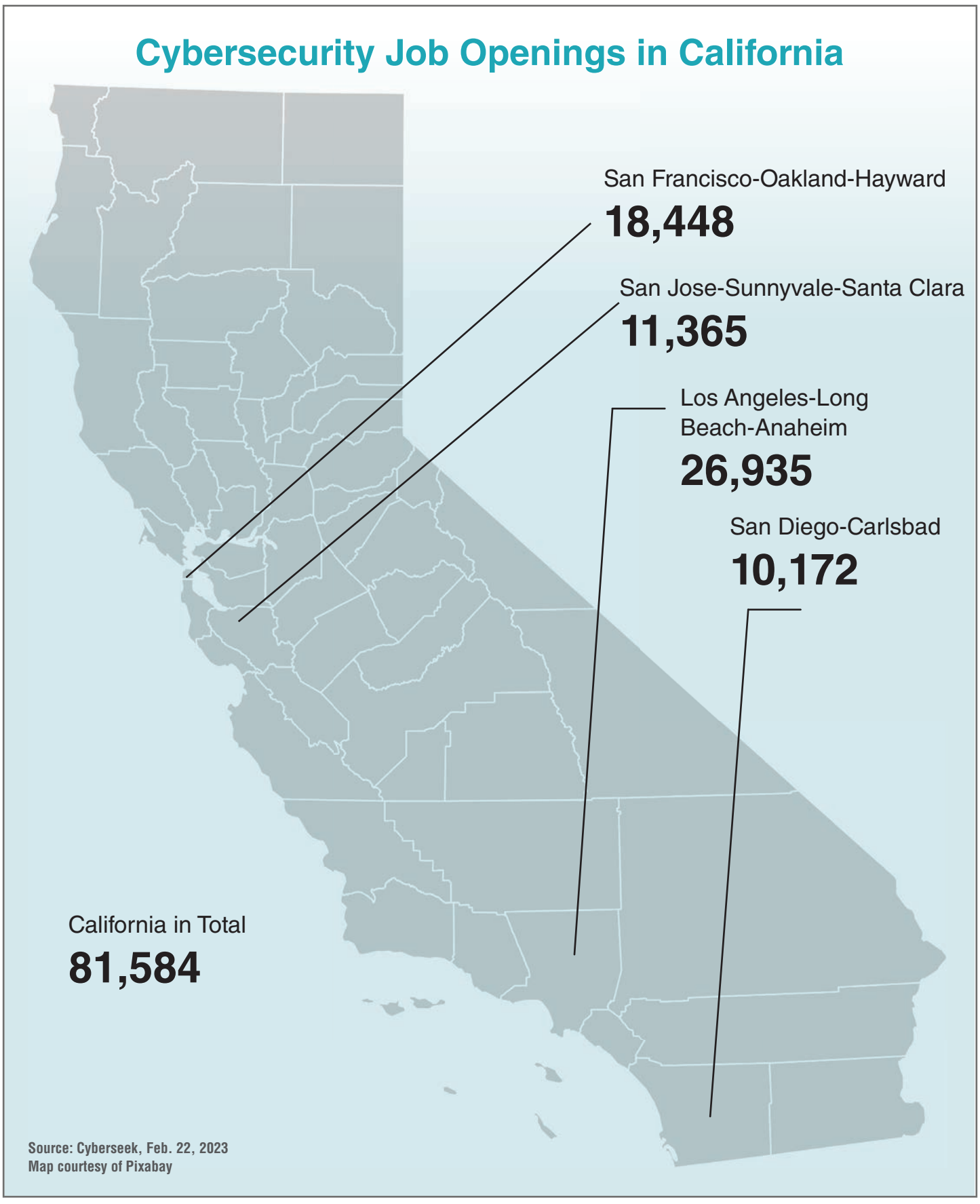
"I think Rich touched on a lot of these concepts as well," Sampo said. "I'm going to reiterate some of those, but I think that rather than to focus on [academia]—and I don't want to take anything away from academia or higher ed—but focusing on industry search, there's a lot of great industry certifications, things like CISSP, GSAC, these are more high level cybersecurity certificates, but there's also some that are more entry level. And I think employers can look at expanding internships and converting internships into potential permanent positions. And so that gives the ability to retain talent.

"So we have all this great talent, or this pool of talent. We don't necessarily need them to go to Silicon Valley. I'm not taking anything away from Silicon Valley, but why not keep them here in San Diego? I think looking at internships and converting some of those internship opportunities into more permanent positions where they can get on-the-job training and creating more junior-like positions that can then evolve into more senior positions is something that employers can do. Adding to Rich's point earlier in the academia piece, career fairs here locally, we've got some great academic institutions like **San Diego State**, who's just built a more recent cybersecurity program.

"The other piece that I have is, there's a lot of local programs that employers can tap into. The **San Diego Workforce Partnership** with **CyberHire** is another great opportunity for employers to

➡ *Cybersecurity page 48*

Cybersecurity Job Openings in California



Source: Cyberseek, Feb. 22, 2023
Map courtesy of Pixabay

Cybersecurity

➡ *from page 46*

cast that wider net. And then the other component is, San Diego's such a great place, right? Aside from academia and some of the organizations that we have here, we also have great military bases, with a pool of individuals that have got some level of training and leveraging those would be phenomenal. And I think organizations or employers need to look at all the different options and look at the wider pool of candidates. And I think that will help cast that larger net and retain great talent, because there is a lot of great talent here in the area."

"Fabulous suggestion. Thank you so much, Miguel," said Easterly.

Think Differently

"So, you know, homogeny is the cyber criminal's best friend, and still only about a quarter of the cyber workforce includes women, minorities and neurodiversity," she said, turning to **Eric Basu**. "Eric, how can we bring more diversity to the cyber talent pipeline to broaden our collective defenses?"

"I actually love that quote, Lisa," Basu said. "I think it's perfect, because the more that you know your defenses are predictable and your programming is predictable, the easier it is for the script kiddies and for AI to be able to get in there. If you have unpredictability [you make it more difficult]. And that comes with diversity of thought, which comes with the diversity of a workforce. I think that's a very timely topic. We actually built Haiku specifically to address that. When we built it, I looked at the other ways that are out there for training. And again, nothing could take away from a higher degree. There's definitely a place if I'm hiring somebody to move into management to have a bachelor's and a master's degree. These are important things. There's a lot of value behind that.

"But to fill the 3½ million unfilled jobs, which you're projected to get to 6, we're not going to get there if we're trying to require everyone to get a bachelor's degree. It's just too hard.

"The lack of diversity in cybersecurity: women only comprise 24% of the cybersecurity workforce. Why is that? Latinos, only 4% of the cybersecurity workforce. We work very closely with **Raices Cyber** which is a nonprofit group designed to increase the number of Latinos in cybersecurity. [The organization's website is raicescyber.org]

"As one example, we built World of Haiku as a roleplaying game. One of the reasons we did that is that 60% of roleplaying game gamers are women versus 24% in the cybersecurity workforce. Videogames cross every demographic, every gender, race, income demographic. People love to play videogames. There's a great book by **Jane McGonagal** called 'Reality Is Broken.' It explains why we like videogames. And rather than telling people they should play less videogames, telling they should play more, they should make real life more like videogames, because it appeals to the basic tenets of what we think as humans. I think in order to be able to do that, it's more than just taking something that somebody doesn't want to do already, putting it in front of more people who don't want to do it and saying, 'OK, now you need to do it more because we need diversity.' That's silly. It's really going to people who aren't in the field that you're in and saying, 'What do you want to see? What would make you want to do this as a job?' It's not just telling them how much money is in it because everybody knows how much money is in it. What will make this easier for you to be able to get into?

"So that was a bit of a long-winded way of saying, we've got to change the way we do it [train people]. And that's exactly one of the reasons we built Haiku. We built Haiku to be able to bring more people into [cybersecurity] by appealing to the way they want to learn instead of shoving an old, traditional learning way onto them."

> **"I love the fact that my son comes to me and says, 'Is it OK for me to download this? Because I know I need to be thinking about cybersecurity.' And he's 9! So we want to start to integrate that into everyone's thought processes, because again, as everyone on this panel has talked about, cybersecurity really is everyone's business at this point."**
>
> LISA EASTERLY

Like an Online Map With Career Direction

Easterly turned to **Richard Portelance**. "For those in our audience that we've inspired to join the fight, from transitioning service members to students, to seasoned professionals with sights on the next level, Rich, how do they get started?"

"They can get started by going to CCOE [sdccoe.org] and using the career map that's plugged in there." Portelance said. "Journeys Map powers that opportunity.

"And what we're trying to do is fill the gap. There's a gap between the training, the actual jobs and the people who want to get there. And so, we're trying to partner with groups like CCOE to create that conduit so that people who are looking for opportunities, if they're working at a company and they're not sure how to get training, they can use the map, they can have their professionals or the students can come in and use the map and find the skills gap.

"That's the first piece of it: Where am I lacking? What do I need to be ready for that particular profession? And then how do I gain those skills? And as these guys pointed out, it could be through some training, it could be through a college course, it could be just on-the-job training, and then they can evolve into those new roles. And I love what Eric was just saying, and actually I think it was Miguel, you were talking about the younger professionals coming in and using those interns and then building them up over time. So, I would reiterate that point as we're talking about how do you get there, use the younger people that are available to you. And if you have an internship program with a local school, that's a great way in which to build a pipeline of talent over time. So, one of the ways we talked about was contacting CCOE, using the mapping function to find skills gap, getting in touch with the people within your community and using the resources at hand in order to build up a stronger team.

"We're very excited," Easterly said. "The map is now in its sixth year, completely free to users. It gives you an opportunity like a Google map. 'I'm here, I want to get there,' and it includes everything from all of the different types of education certifications, hands-on learning like Haiku, as well as determining what your skills and interests are and where that aligns in the cybersecurity realm.

"I always say, I'm not a cybersecurity technician, but I live and breathe cybersecurity. My background is finance and economics. There is a place in cybersecurity for everyone. We need folks that are great communicators. We need folks that are good problem solvers. We need good collaborators. So it's really an exciting field to be able to join at a time where it's just incredibly in demand and every single industry needs it. So if you want to be in medicine and you can't deal with blood and you want to help folks, cybersecurity is a great place to get in."

Portelance interjected: "I would add that, Lisa, we have over 30,000 skills represented on the map now. So think about where you are traditionally, with a system that might have 300 skills represented that match you up to jobs. We've expanded that greatly. Now we're offering over 30,000 skills, so that's going to make it much more finite. And for career fields like cybersecurity, that's super important because you need to get specific with those skills. And then we have a matching technology so that you can see the gap that's existing between where you are today and where you need to get to. And then we can match those up to those learning opportunities like you just pointed out, that are all localized. So there's a lot of opportunity out there and a lot of new technologies. It's just kind of identifying and finding where they are and taking advantage of it."

"Absolutely," Easterly said. "And I think what's helpful for employers as well is this is an opportunity to upskill exactly as Miguel said. You've got folks that are part of your corporate culture that you spent the time and energy to bring into the team. This is an opportunity to look for some of those folks that might be able to upskill into some of these additional cybersecurity roles."

Parting Thoughts

At this point, Easterly asked each participant for a final thought about the current threat landscape and workforce trends.

"It's a thought I've used before on other panels," said **Eric Basu**. "For a business, if you're trying to fill your positions, don't advertise an entry-level position that requires three to five years of your experience. It's become a meme. You've got to be willing to take people and hire for skills rather than hire for the degree that somebody chose when they were 18. And that's how you're going to start filling that in there. It takes a little more work and it takes a little more confidence and knowledge on the part of the business, but that's how we're going to be able to close part of this workforce gap."

"I would say that you have to look at nontraditional pathways to careers," **Richard Portelance** said. "As Eric was just saying, you need to look into the high schools, you need to look into the community colleges. Find people that are interested in the topic. They don't necessarily have to have a four year degree to be a contributing member of your team. And most likely, those people that are nontraditional are going to offer a very unique perspective on cyber. So definitely look outside the normal boundaries to find talent."

Miguel Sampo offered a last thought: "You know, Lisa, I love the quote that you say, and I think cybersecurity is everybody's business. And I truly feel that in today's modern era, the technology era, it's not just on the professional level, it's also on the personal level. Safe computing, right? Understanding what app you load on your smart device, on your home PC. The responsibility isn't just at protecting the workforce or safe computing practices in the workforce. As an individual person, protect yourself, take care of yourself, educate yourself. You download an app. Understand what are the drawbacks of an app or how do you use that app efficiently and correctly. In this world, the threat landscape is evolving. And it's not going to go away. At least not in my lifetime. And so I think understanding how to be diligent, how to be vigilant around your safe computing practices is the note that I'll leave everybody with.

"Stay safe."

"Yes, I think every family's motto should be Think Before You Click," **Lisa Easterly** said. "And we start them young. My final thought is, it is not too early to start talking about cybersecurity with your children. I love the fact that my son comes to me and says, 'Is it OK for me to download this? Because I know I need to be thinking about cybersecurity.' And he's 9! So we want to start to integrate that into everyone's thought processes, because again, as everyone on this panel has talked about, cybersecurity really is everyone's business at this point. And it is all of our responsibility to make sure that we help keep all of these critical infrastructure pieces safe as well as all these key industries safe, and then all the way down to our communities and our families.

"Thank you so much. This was such a fun discussion. I love speaking with you guys. You've become fan favorites. Great, insightful conversation today."

Easterly said businesses as well as job seekers can visit the CCOE website, sdccoe.org, to find many of the resources discussed by the panel. "There is lots of information and a lot of free resources there for the community."

Easterly concluded with a thank you, and said the next **San Diego Business Journal** Cyber Trends panel discussion will be in the spring. ■