HELP SAN DIEGO LEAD THE CYBER CHARGE

Cyber Center of Excellence (CCOE) is a non-profit that mobilizes businesses, academia and government to grow the regional cyber economy and create a more secure digital community for all.

We invite you to join us in advancing the region's cyber workforce, infrastructure and global market share for a robust industry that already **supplies 24,350 jobs** and **invests $3.5 billion** into San Diego's economy.

Get involved at **sdccoe.org**.

Lisa Easterly, CCOE President & CEO

ACCELERATING THE CYBER INNOVATION ECONOMY

Cyber Center of Excellence

CCOE

IT Pros Share Tales From the Cybersecurity Trenches

CYBERSECURITY: Roundtable Convened by CCOE and SDBJ Offers a Glimpse of San Diego's Future

■ BY BRAD GRAVES

Five of the region's IT leaders gathered on a recent Friday to talk cybersecurity — about staying safe in an environment where opportunists and bad actors lurk.

They shared stories and perspectives as part of the Cyber Trends 2022 series of discussions. This talk, like the two before it, was presented by the **Cyber Center of Excellence** and the **San Diego Business Journal**.

For the August talk, participants offered stories from the trenches.

That was only part of the discussion, however. Several had new initiatives to report.

Cybersecurity will be part of the Innovation District that **San Diego State University** plans to build around its new stadium in Mission Valley. The university is also adapting its cybersecurity curriculum to the times and to emerging threats.

The **City of San Diego**, for its part, plans to open a Regional Cyber Lab as an aid for businesses and communities.

Panelists for the August talk were **Ian Brazill**, program manager in IT operations management and compliance with the City of San Diego; **Mark Compton**, a **U.S. Navy** civilian who is command information security officer (CISO) with **NAVWAR** (the Naval Information Warfare Systems Command; **Miguel Sampo**, senior director for the Cyber and Intelligence Group with **RiskRecon**, a **MasterCard** company; and **Jerry Sheehan**, vice president and chief information officer at San Diego State University.

As usual, the talk was moderated by **Lisa Easterly**, president and CEO of **Cyber Center of Excellence** (CCOE). The organization is 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.

MODERATOR

LISA EASTERLY

Lisa Easterly is 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. Previously Easterly was vice president of marketing and senior adviser with the San Diego Regional Economic Development Corp. and a founding member of Cleantech San Diego. Prior to that, she held business development jobs with San Diego area law firms. Easterly received her MBA from the University of Florida.

A fourth panel discussion is scheduled later in this year. Special coverage of Cybersecurity Month, taking in the 2022 Cybersecurity Stewardship Awards, is planned for October.

Bad News and Good News

Easterly kicked off the panel discussion by noting that cybersecurity is everyone's business. The **FBI** reports a 300% increase in cybercrimes across all industries since the pandemic began, with the average cost of a data breach climbing over $4 million, according to the **Ponemon Institute**.

"More than half of these costly attacks are aimed at small and medium-sized businesses, and that is our region's economic engine," she said.

"Now pair that with the global shortage of cyber professionals to thwart these attacks — to the tune of about 3½ million globally, and more than 60,000 openings here in California — and it becomes mission critical to integrate cybersecurity into our daily practices.

"The good news is San Diego is leading the charge with more than 870 cyber firms and the U.S. Navy's Naval Information Warfare Systems Command. This 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, or for all of you Marvel fans out there like me, 23 Comic-Cons. This collaborative ecosystem is developing new technology, defenses and cyber warriors to combat the ever-evolving threat landscape."

She then introduced the theme of the day: lessons learned and best practices from some of the most under-fire industries — like defense, education, financial services and the public sector — that can be applied to all industries.

Following a round of introductions, Easterly kicked off the discussion.

By the Numbers

Economic Impact of Cybersecurity Cluster on San Diego, Annually

$3.5 Billion

(The equivalent of 9 Super Bowls or 23 Comic-Cons)

Source: CCOE

Navy's IT Experience May Seem Familiar

Easterly noted that the United States is the No. 1 target for cyberattacks, according to **Microsoft**. San Diego is home to the largest concentration of military assets in the world.

She asked Mark Compton to provide a big-picture look at defense cyber operations, including an unclassified view of how the Navy handled a recent vulnerability, and lessons learned.

➡ *Cybersecurity page 26*

THE PANELISTS

IAN BRAZILL

Ian Brazill is a program manager with the City of San Diego's Department of Information Technology. He is currently helping to lead the city's effort to design, build and market the San Diego Regional Cyber Lab. The goal of the lab is to provide the greater San Diego region with a more collaborative cybersecurity awareness effort through the provision of extra tools and intelligence and a more trained and capable workforce. His team consists of cybersecurity experts, academics, local CEOs and other public officials working together to enhance the entire region's cybersecurity resilience.

MARK COMPTON

Mark Compton is command information security officer — the military equivalent of CISO or chief information security officer — for NAVWAR, the Naval Information Warfare Systems Command. The U.S. Navy command identifies, develops, delivers and sustains information war-fighting and enterprise capabilities and services to enable operations in war-fighting domains from seabed to space. The San Diego-based command has approximately 11,000 military and civilian personnel and a budget of $9 billion. It has more than 350 applications, systems, networks, data centers and services capabilities that it needs to protect.

MIGUEL SAMPO

Miguel Sampo is senior director with MasterCard, working for the cyber and intelligence division under the RiskRecon group. His career in cybersecurity spans 24 years. "I think I've walked almost every single discipline of the cyber realm, from endpoint protection to cloud security, to SaaS to perimeter — you name it," he said. Over the last four years he has worked in third party risk management, vendor risk management and supply chain management. He specializes in doing security risk assessments for third party and fourth party vendors. His organization generates a cyber score, similar to a credit score.

JERRY SHEEHAN

Jerry Sheehan is vice president and chief information officer for San Diego State University, representing campuses in San Diego and Imperial Valley as well as the university's new campus in Mission Valley. SDSU is "really at that epicenter of looking at how we create the knowledge that's necessary among our 40,000 students to prepare them for the complexity of the cyber world that they live in right now," he said. The university is also trying to meet workforce development needs and is pursing fundamental research through partnerships with many organizations, including NAVWAR.

The Aztec Experience

The roar of 35,000 fans will be felt on September 3 at Snapdragon Stadium for the Aztec Football season opener. This is the first development of SDSU Mission Valley and will unlock other plans for the site to further connect the community, industry, entertainment and research in a leading-edge environment.

Learn more at SDSU.edu

SDSU | San Diego State University

Cybersecurity

➡ *from page 24*

"I think what I'll do is describe very briefly what the hierarchy is when it comes to getting directions on addressing vulnerabilities and incident response," Compton said.

"When it comes to defending the **Department of Defense** information networks, direction comes down from **U.S. Cyber Command** to lower echelons. And a major part of their mission statement is to direct, synchronize and coordinate cyberspace planning and operations. And so that command seeks to mitigate risks indirectly by increasing resiliency in DoD systems against all threats."

It is a top-down system, with top leaders laying out a plan or defense overall, and providing direction and information on how that's to be carried out, Compton said. A directive may come down saying, in effect: "Hey, we've got vulnerabilities out there that are of major concern, and we need you to execute cyber defense actions in order to be able to protect against those vulnerabilities."

Top leadership might also notify NAVWAR of some sort of breach.

"And of course now, we're all about defending our over 350 information systems that we design, test, deliver and maintain," Compton said.

"And we not only have those systems we deliver out to the fleet, but we hold the whole research, development, testing, engineering, and network laboratories. And so we take this very seriously, particularly when it comes to vulnerability patching. So we get these top-down directions; they come into my office and I've got a very small team. We will take these directions and go ahead and triage them, figure out what it's all about, where it's going to apply across our organization and get the information out to the organization, so everybody — all our cybersecurity action officers across these systems — know what's coming down. Plus they get additional information from us if it's specifically for their applications. And so, there's a lot of challenges that come along with vulnerabilities, carrying out vulnerability defense."

NAVWAR has "pretty complex systems that we deliver for the naval forces," the executive said. "And so when we get these patch directives, we have to do a lot of analysis on how we're going to incorporate those patches on these commercial systems, especially into [those] that are part of our systems and make sure that the work that we do on those patches is not inadvertently causing things to go bad. Because the last thing you want to do is deliver a patch out to the fleet that has a chink in it and find out that now a weapon system is not doing what it's supposed to do. So we've got very strong engineering in the organization that makes sure those kind of things don't happen."

Getting People Organized

"I'd say another thing that we face is getting the information out and getting people organized. And so one of the things that I can talk about is a particular case that we had last year. We received a notification, a direction out of Fleet Cyber Command, to identify this particular vulnerability, where it was inside of all of our systems, and then to go ahead and carry out remediating actions, awaiting the vendor having a patch that we could apply. So it's multi-tiered kinds of actions. And so the first thing we did was we brought our team together to triage this. We got the word out to everybody that this is coming across all of our systems, and we're talking about dozens of cybersecurity action officers. And then we started to see, OK, so where is this targeted at? One of the things we found on this particular vulnerability is it was very widespread across our systems because of the nature of the product that it was on. And so that started opening our eyes, that this was bigger than the average one. And the other challenge we found was that we also had data centers where we host what we call mission owner applications.

> **'We're all about defending our over 350 information systems that we design, test, deliver and maintain. And we not only have those systems we deliver out to the fleet, but we hold the whole research, development, testing, engineering, and network laboratories. And so we take this very seriously, particularly when it comes to vulnerability patching.'**
>
> MARK COMPTON

"And there are hundreds of those. And each mission owner is responsible for carrying out, their vulnerability remediation on their particular systems. But because they're part of a data center, it's like a link in a chain: you get a break in one and it causes a problem across the whole data center potentially. We put the word out."

The challenges, he said, were:

- Having a broader set of people that the office had to communicate with, a set "that went beyond our normal communications. And this is out to all those other mission owners. So making sure that we could bring them into the conversation."
- Getting coordination on this activity and "making sure that we got that coordination done well." In a worst-case scenario, some participants would have to be cut off of the network.
- Making sure that everybody knew what to do as it's going through this patch development phase.
- Executing, tracking and reporting up.

The Three C's

The executive then went through what he calls The Three C's. They are useful for defensive operations, in preventing an incident or responding to an incident.

"One is communication, making sure you've got your communications path set up ahead of time," Compton said. "You don't want to be figuring this out in the midst of the battle and that everybody understands what those communications paths are. They've got the access to those communications paths and they know how to dial in."

He continued: "The second C is coordination. It's one thing to have the communications path, but it's another thing to have it coordinated to where everybody knows who needs to be, where and when, and is prepared because they've received the information and know what they need to do.

"I'd say the third C is collaboration. And this is exceedingly important because you find that there are different levels of expertise in your systems. And so you get together super experts with experts to help solve problems and bring everybody along in order to remediate the incident."

At this point, Easterly noted that San Diego is a global hub not only for defense, but high-tech development and manufacturing, renowned education research institutions, as well as tourism. "This creates an unfortunate bullseye for damaging attacks to our region."

Regional Cyber Lab Comes Into Focus

She then turned to Brazill of the City of San Diego and asked about the leading threats he is seeing at the state and local government levels. She also asked how the new San Diego Regional Cyber Lab is working to mitigate them.

"About two years ago, we conducted an informal regional survey of a lot of public and some private institutions across the region," Brazill said. "We've come to understand at least some of the more common issues that especially the small and midsize public agencies seem to share. And so we asked them, what are some of the biggest challenges to improving cybersecurity at your own agency? And it seemed that, across the board, one of the more common responses was that there was just simply a strong desire to increase the sheer quantity of dedicated cybersecurity staff in their organization and along with that, all of the training necessary to get that staff up to speed.

"And so I think at a certain level, it's a numbers game, that we all just want to get more cybersecurity staff on board, with the second biggest response from a lot of these organizations was again, related to staffing, but more specifically staff expertise," he continued.

Brazill said when looking at small and medium-sized public agencies, a lot of them have a "more generalized IT staff" that serve a variety of roles across the organization.

"So you might have an individual that is your primary help desk contact, but they're also dealing with networking orders and they're dealing with cybersecurity tasks as well," he said. "So they're great generalized staff, but I think a lot of what these organizations are looking for is, at this point, staff with expertise in a particular area."

The challenge, Brazill explained, is that the industry is often in a "sort of negative unemployment" where there are more jobs available than there are people to fill them.

Another challenge that organizations are facing is "a response bandwidth or even a preparation bandwidth," he added. "You only have so many staff on hand to deal with whatever's getting thrown at you and to prepare for what you expect might be thrown at you in the future. And so again, a lot of it comes down to staffing."

Another major challenge organizations face is competing business needs and funding priorities.

"I think we can all agree that there's only so much budget in any given organization and you're always fighting to get whatever money you can," Brazill said. "So getting as much as you can into cybersecurity as possible is really important to all of these organizations and a constant challenge for them."

Brazill pointed out that Cyber Lab is developing a number of ways to meet these challenges that will benefit the entire San Diego region, such as stablishing partnerships with educational institutions in the area.

"In fact, several of them actually reached out to us before we reached out to them," he said. "They told us, 'Look, we have a number of students who need capstone projects, they're working in cybersecurity. Do you have other organizations that you've networked with across the region that might benefit from a free penetration test, a free vulnerability assessment from a group of students that need to put a project together?'

"And so we're hoping to build some of those bridges, especially for those smaller organizations that might not have the capacity to perform all these services themselves, and also perhaps not the budget to also pay for all of these services, as frequently as they'd like. We could leverage some of the student populations in the city," he continued.

Cyber Lab is also developing a number of cyber ranges, which Brazill likened to a shooting range for a police department.

"It's a safe, walled-in area. You can break things and rebuild things and you're not going to harm your organization," he said. "And so we are building a cyber range that's going to be accessed remotely or within our physical lab space downtown, and all of the trusted partners that we have are going to be given access to test their own organization's tools, and their own teams' capabilities to protect their own organization against a variety of different circumstances."

Intelligence: Expensive But Within Reach

"We also know that threat intelligence feeds are really important — and sometimes they are also incredibly expensive," Brazill said. "And so we've been lucky enough to get some grant funding from the federal government and we have purchased a variety of hardware and software, but some of the software we've purchased is licenses for very pricey threat intelligence feeds. And what we'd like to do is provide those licenses temporarily to a variety of organizations across the region so they can at least get a sense of what might they get out of a tool like this, so that they can test it out, no cost to them, so that in the future, hopefully more organizations across the region will use more products like this."

He went on to describe the organization's physical lab space in downtown San Diego, with a variety of workstations including Macs and PCs. "We've purchased a variety of forensics, hardware and software that are used by forensics experts today," he said. "So if you're an organization that works with forensically sensitive data this would be a great opportunity to get some hands-on experience with these products perhaps before your organization buys them yourselves. And then we're going to have a server rack with a bunch of servers in it, and we can build to your heart's content, whatever you'd like to see in there. And if you'd like to bring your organization in and play some scenarios, maybe some attack and defense to build a version of something from your own institution, and then test your team's abilities to defend themselves against potential attacks, [we] can run all sorts of scenarios."

He continued: "We're hoping that just having that space that we want to emphasize to the region, it's really owned by everybody. We hope that they start participating in

➡ *Cybersecurity page 28*

Cybersecurity

➡ *from page 26*

events here and perhaps if you want to hold a training session downtown with your team or with several different organizations, have some roundtable discussions about regional issues that we need to work on together, we're hoping that the physical lab space will provide opportunities like that."

Changing Old Ideas

"Oh, we're so excited for this new resource," Easterly said. "CCOE has been in the trenches with the city and many partners through the development. And we can't wait to bring this resource online for the region this fall.

Easterly noted that education and research is no stranger to cyberattacks, facing about a 75% increase since the pandemic's digital push, according to **Check Point Software**. **Cyberseek**, for its part, reports that California is facing a deficit of 60,000 cyber professionals to thwart such attacks. "So Jerry," Easterly said, turning to SDSU's Sheehan, "can you speak to the value and the types of programs available to increase cybersecurity training and preparedness across an organization?"

"I think it's really important as we think about the framework for that question that we approach it from thinking about the continuum of need that is out there," Sheehan said. "And really, as we think about the opportunities and the challenges going back to even the complexity that Mark talked about, you just see an awful lot of need for us to be producing information that gets quickly diffused.

"So at San Diego State University, to approach that continuum, there are three things that we're focused on. First of them is the area of credentials. So these would be non-degree knowledge ways. And I'll talk a little bit more about that. The second, the degree programs that are formal, and then the third being our research activities. And I think as we go back to that mantra of CCOE, that cybersecurity is everyone's business. In order for it to be everyone's business, we have to be producing the right ways for people to get the information that they need."

At the university, the traditional model used to approach the diffusion of knowledge has been a traditional course that led to a degree. After a few years, Sheehan said, "you were ready to go."

In the San Diego region and across our society, he continued, "we see things where knowledge needs to be more discreetly gotten into the hands of folks so they can practically make those changes that are going to be needed to secure their environment. We've innovated in that area, through our Homeland Security program and our Global Campus in creating cyber certificate degree programs that allow you to assess the knowledge that would be necessary to become credible as someone who could respond in these areas.

"But I think what you're seeing right now in all of higher education is an easing of that idea that you have to get to a degree completion in order to have new knowledge that's going to be actionable. So from San Diego State University, you're also going to see aggressive moves into stackable credentials, things that would allow you to have the information that you need to know just in time. And as we think about the community threats that are out there, we have a broad area, from those who are in the supply chain to even individuals who are at home, really cybersecurity is a lifelong learning challenge. If you think about where most of us started our lives, where passwords were things that were only reserved for people who had access to certain types of documents to now, to all of us, having them, multifactor authentication, being something that is now diffused."

Not an Add-on

"I also know that San Diego State University is making aggressive moves into offering a formal degree program ...," he continued. "Cybersecurity can't be the thing that you think of in addition to your job, it has to be the thing that is the way that you do your job. And one of the transformations that we're really focused on in the curriculum at San Diego State University is to make sure in particular, in the science, technology, engineering and mathematics disciplines, that cybersecurity and cybersecurity awareness is something that's being taught as a component of our courses. So it's not as if you go through the public health school, get your degree or your masters of public health, and then after that, think about how cybersecurity might apply to the work that you're doing.

> **'It really sounds scary, but the reality is that if we take a couple different steps ahead of time and do this early, rather than when the snake bites us, we're going to be ahead of the game.'**
>
> MIGUEL SAMPO

"We want to make sure as folks are getting those degree programs that cybersecurity in multiple disciplines is seen as a component of things. Because I think one of the challenges that we have faced in the past is that cybersecurity was another discipline. It wasn't the way that we executed our disciplines. So that's really another transformation that's going on in the formal degree programs."

Finally, he said, "I think for those institutions in particular, San Diego State, sitting in the trans-border region, our campus in Calexico, we have the special responsibility to think about what research enables us to do. And I want to talk about just a few things there. First and foremost, research in and of itself is creating both new threats and allowing us to create approaches to deal with existing threats in different way. You appropriately talked about as many threats as we face in higher education. Those are persistent, tens of thousands and hours' worth of automated probes.

"And then what we have seen fundamentally is that cybersecurity is no longer something that requires a lot of domain knowledge. When I was a kid growing up, you sort of needed to know how to code and at least have a keyboard that you could get to that would allow you to put commands in before you could become a threat to anyone else. But increasingly in the world that we live, the Amazon-ification of the cyber threat means right now for just a little money, all you have to do is be able to push a button and type in a few numbers associated with where a computer exists and you can begin to target individuals. And I think that speaks to the importance of the transformative research that San Diego State is at the epicenter of."

Put a Plan in Place

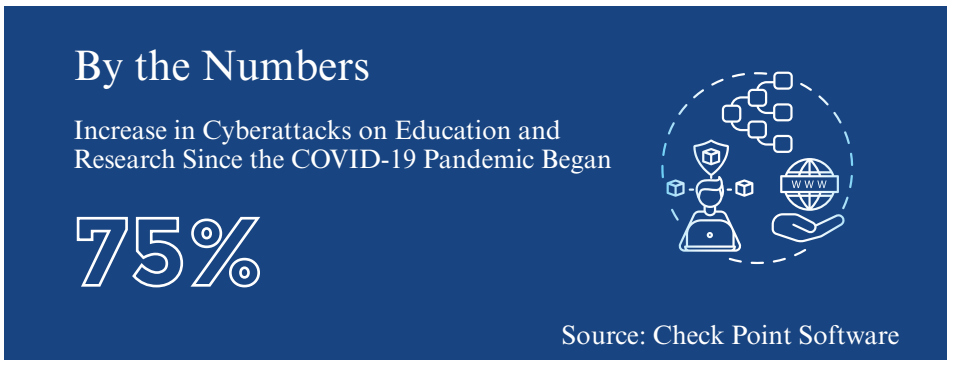
At this point, Easterly turned to Miguel Sampo and noted the "considerable uptick" in supply chain attacks. She added that the average cost of a data breach now has climbed to more than $4 million. "Miguel, what best practices do you suggest for these small to medium-sized businesses that are often the entry point and unfortunate casualties of these attacks?"

"So super excited, right?" Sampo responded. "This is a great conversation, a lot of great soundbites that have come out of here. Ian talked about talent, talent acquisition and the shortage of talent in the area. And having the right professionals. Mark talked about vulnerabilities and how to understand the existing risk to today. Jerry talked about cyber excellence and some of the other things that are going on around training."

He continued: "We can infer a couple things. So there is not one best practice, right? This is what we call security in layers, yesterday's security landscape, or cybersecurity landscape. And the processes of yesterday are not the same today. They've evolved significantly – the days of only having an antivirus program on your endpoint and a good perimeter security, like a good firewall, those days are long gone."

He spoke about cybersecurity emergency drills. "We have red team, blue team, purple team … we practice for when zero-day comes and we have that attack. What do we do? What does that process look like?

He continued: "What I would tell you is that the best strategy is to build a plan. If that day comes, what do we do? What is step one, what is step two, what is step three? Who do we call? Who's the next person in the calls? But from a more tactical perspective, there's a lot of different things that we can do.



Evaluating Supply Chain, Doing Drills

"And so the first thing that we want to do is make sure that we have all of these drills or exercises that we've talked about in place to some degree. More specifically around the supply chain itself, it starts with being proactive. I would tell you that so many companies will react when something happens. And there's so many tools and solutions that we can use today that are cost-effective to help us get an understanding or visibility into what the inherent risks are that exist for an organization. But, the days of just protecting my organization, those days are gone. That's not enough anymore. We are connected in today's modern world in so many different ways to so many different vendors. And when organizations think about their vendors, the first thing they think about or myopically, they're only thinking about my IT vendors."

That is wrong, Sampo said. "You've got a lot of different vendors. You've got the vendor that supplies the paper and pens and ink to your company, the guy who's dropping off uniforms and cups and everything else for the break room, you've got HR applications. You can name hundreds, if not thousands of different vendors that we're connected and dependent upon, and that we're sharing information with. If they're not taking the same due diligence that you are, and they're connected to you, and something happens, you've left the door wide open. And so what do we do in this scenario? So there's tons of solutions out there that do cyber scoring and whatnot.

"They're all evolving and they're getting better, but here's what I recommended to organizations: Start by understanding what your inherent risk is. Who are these critical vendors that I'm doing business with and how am I connected to them and what data do they have and what can we do? There are solutions out there that leverage, like Jerry talked a little bit ago, machine learning. Or taking it a step back, AI — that leverage AI that can automate processes that once were a very manual, very heavy resource consumptive kind of scenario or process. We can automate these and use solutions like RiskRecon, for example. And there are other competitors in the markets that can run security assessments, give you visibility into where there's potential risks or gaps that exist with the vendors that you're working with, and then create an action plan," Sampo said.

"Start to collaborate. Communication, I think was brought up earlier, communicating with these vendors about what your SLA [service level agreement], what your expectation is of them and vice versa, and then start to address those gaps. Mark knows this really well. There are over 100,000 known vulnerabilities in the wild. To think that we're going to tackle all 100,000 is probably not realistic because maybe not all 100,000 apply to your organization, but understanding which ones are critical and most important to your organization and understanding where those gaps are, are the first step in prevention. So I would say looking at solutions that can do continuous monitoring to help you understand the cyber hygiene of not only your organization, but your vendors is equally important."

At this point, he stepped back.

"It really sounds scary," Sampo said, "but the reality is that if we take a couple different steps ahead of time and do this early, rather than when the snake bites us, we're going to be ahead of the game. We're never going to be 100% ahead of the bad guys. It's just the nature of how it works. At least that's what I've seen in 25 years in the field. But we can take steps to help us prepare— it's not a matter of if; it's a matter of when — when that day comes, to best deal with that situation.

"Great discussion, gentlemen, about lessons businesses can learn from the cybersecurity trenches," Easterly said. "But let's take a minute to turn the tables a bit. Mark, what are some of the top security challenges that you face as a CISO for the Navy's information warfare systems command and how can industry help?"

It's About People: The Training Component

"I'm not going to be very sophisticated with my first one, but to me it hits the base of everything in cybersecurity. And that has to do with things evolving around our personnel," Compton said.

"When you take in the vendors that support us, we have over 20,000 people that are supporting NAVWAR and carrying out our mission. That's a lot of people, that's a lot of potential links in the security chain that can be broken and you've got a real problem. And so I'd say that the number one piece is making sure that folks are all cybersecurity trained and it's part of their daily function. And it almost has to come without them thinking about it in the way that they operate when

➡ *Cybersecurity page 30*

SAN DIEGO REGIONAL CYBER LAB

LAUNCHING SOON...

With cybersecurity concerns on the rise nationally, the new San Diego Regional Cyber Lab's mission is to help small businesses, government agencies and other organizations bolster their cybersecurity capabilities – and unite our region in the fight against damaging cyberattacks.

The new Cyber Lab will provide the greater San Diego region with coordinated cybersecurity awareness through collaborative access to tools, threat intelligence and a trained and capable workforce.

What does the Cyber Lab offer?

- Collaborative information-sharing on malicious activity and emerging threats
- An online database with the best practices for cybersecurity
- A training environment, with both virtual and physical lab space and ability to host cybersecurity competitions
- A new website with tips, resources and the latest cybersecurity news
- Access to an established network of regional groups and technical committees with like-minded cybersecurity goals

Check out the new San Diego Regional Cyber Lab at: **sandiego.gov/cyber-lab**

And, as always ...

Stay Secure, San Diego!

Cybersecurity

➡ *from page 28*

they get onto our networks. And so the Department of Defense has annual cybersecurity training requirements out there.

"And so making sure that that training is available and making sure that everyone gets their training every year, so they are reminded, one, what are the baseline things that they do? And then two, when there are new particular issues out there in cybersecurity, that they are aware of those issues as it affects them. It's so incredibly important that we make sure that the folks that are going to be touching our systems down to working with the operating system, managing code, et cetera, that they have the necessary training and certifications to work on those systems, that they're current enough that they're not going to cause a problem because they're lacking that training. So privileged access [is] very important."

He spoke of having "cybersecurity to the core." The need, he said, is absolute. "And this gets down to folks like the developers, the program managers, engineers, et cetera."

'Spillage' and Mom's Laptop

"Also out of my office, we get into what do you do on a personnel level," Compton said. "We have spillages that do happen, going from one domain to another occasionally. I hate to say it, but it does occasionally happen. Most of them, fortunately for us, come from outside the organization where we get an email from somebody that they had information in there that shouldn't have been in at that particular security level. Well, there's cleanup that has to happen on that. So we work on the spillage cleanup out of here and make sure that we contained the problem."

'Cybersecurity can't be the thing that you think of in addition to your job, it has to be the thing that is the way that you do your job.'

JERRY SHEEHAN

Another matter is proper use of equipment.

"People mess up," Compton said. "The one I like best— this happened not just a small number of times with people working during COVID — they left their laptop sitting there and their little girl comes over and she plugs in her mobile device to charge it on mommy or daddy's laptop. Bingo. Fortunately we have network systems that immediately detect there's been an unauthorized device connected up. Now we have to go ahead and make sure that the individual is informed, their supervisor informed. They get remedial training to handle these particular situations. I have always laughed about that one.

"And then there is an inappropriate access to the websites and downloading information. Fortunately over time, I think we have rooted it all almost completely out of the problem space by education and by administrative responses to folks that are improperly behaving on our network. So that personnel side is so core to everything.

"Let me say what our challenge is there. The government, we seem to have a lot of old processes and tools in order to be able to do our administration of things on a personnel level. We really do need to have more automated systems to be able to carry these functions out. And so we're trying to work with that. We're moving a lot more toward robotic process automation, and utilizing enterprise capabilities for managing these things. But we need more help from industry on developing capabilities that help us reduce the amount of time it takes us to carry out these functions and ergo it's going to reduce costs and it's also going to reduce vulnerabilities."

Compton continued with a technical discussion of a compliance-based system versus a "true risk" system. "Our organization as well as the Navy as a whole is working very hard in this arena to get us more risk-based instead of compliance-focused." He also touched on situations where contractors have to safeguard government information, as well as Cybersecurity Maturity Model Certification requirements.

Age-Appropriate Education

At this point, Easterly turned to Ian Brazill of the City of San Diego. "What would you like to see from the broader community and cybersecurity industry for the soon-to-launch San Diego Regional Cyber Lab to foster greater regional resiliency?"

'I think our goal is to have San Diego thought of as a holistic region that is cyber mature. We all have notions about what Silicon Valley communicates as a region. I think in the same capacity, we want San Diego to be representative of a certain level of tech maturity.'

IAN BRAZILL

By the Numbers

Deficit of Cybersecurity Professionals in California

60,000

Source: Cyberseek

"So there's a few different things that we would love to see," Brazill said. "For starters, I think in this day and age, increasing somebody's level in cybersecurity maturity, or even just sort of tech maturity in general, couldn't start sooner. So if you have some young ones, I think even basic education on how computers work, how does your home network work, what's a password manager, what makes a good password, things like that up into better cyber education for high schoolers. I think a basic computer science course for individuals that age is seemingly critical. They're going to be entering the workforce soon. We have a lot of jobs available and there's going to be even more in the future. I think we need to start pumping in more education into that population."

A City Lab's Potential

"So obviously with the cyber lab, we want to create a more collaborative region in general," Brazill continued. "And so we would like to see organizations reaching out to one another. And we are happy to be that sort of glue that binds them together to bridge those communication divides. We would like to see, let's put on some hackathons, some capture the flag events like Miguel was saying: some red team, blue team, purple team, whatever you want to call it. Let's put on some physical events where we all work together, we network a bit more, we have those communication channels open so that if and when something happens to any of those organizations, they don't just have to rely on themselves, but they can reach out to the greater region as well, because I think at this point we are all networked together and we have to rely on one another.

"And also, a lot of small and medium size organizations have outside resources for cybersecurity consulting. So oftentimes you could get some state and federal consulting work done for your organization. The problem being that a lot of these organizations still don't have the resources to actually implement the new programs that they might be recommended without some additional physical, boots-on-the-ground assistance. And so I think if state and federal agencies could help sort of increase the overall cyber maturity of our region as well, by not only assisting with the identification of potential vulnerabilities, but also helping with the physical remediation of those vulnerabilities as well, [that] would be a great help.

"And then, just selfishly for the cyber lab, I think our biggest desire is just for the region to participate with us. We are still on the early stages. We're still buying all of our equipment. We're still getting off the ground. But when we're off the ground, we'd like to see more organizations reaching out to us. We have a quarterly newsletter that we just started. We'd love to see them reach out to us for their own articles: What did another municipality near us just do to increase their cyber resilience? What new tools are they using? So contribute to our newsletter. At the very least follow it. So if you'd like to contact us, we have a general email: SDRCL@SanDiego.gov. That's just San Diego Regional Cyber Lab abbreviated. We can get you on our newsletter, get that in your inbox every quarter. We're also trying, to the best of our abilities, to establish as many different communication channels as possible that might work better for different types of organizations. So, LinkedIn groups, for instance, a private LinkedIn group with different organizations in the region might offer the ability to communicate with one another in a way that's a little bit less formal than full-on email threads. Email's great, but perhaps it doesn't work for everything. Organizations can immediately get others' contact information through LinkedIn without handing out your email to the world. So we're finding a variety of ways like that to hopefully help the region out. And we're just hoping that other organizations are willing to participate as well."

Mission Valley: 'A Living Laboratory'

Easterly then asked Jerry Sheehan about SDSU's new Mission Valley campus. How, she asked, will it help the region get ahead of bad actors? And how can local businesses get involved?

"Let's talk a little bit just about what Mission Valley is as a campus for San Diego State University," Sheehan said. "So a half billion dollar investment, all of that not coming from tuition, but coming from other means as we look at growing out the opportunity. When you look at the innovation area that's in Mission Valley, you're really looking at three distinct areas. First and foremost, given that we are almost at the start of another football season, is the 35,000-seat Snapdragon Stadium. And I think that speaks to the intersection of private sector interest, in particular high tech partners at Qualcomm, in what can be the innovations that will happen in San Diego, in particular, in Mission Valley. Outside of the stadium, you also have 4,500 residential housing units that will go in — 10% of those being targeted to help us address the affordable housing crisis in San Diego. And then you've got 1.6 million square feet of research and innovation space. And in addition to that, you've got about 80 acres worth of parks that also fuse in the idea that this is a real area, that folks will live, work, play and be educated. So you've got about 95,000 square foot of retail space."

SDSU's potential to transform that area of the city is great, he said.

"So what does this mean for our cybersecurity opportunities?" he asked. "Well, I think first and foremost, it's really important for all of us. We certainly love San Diego given we're here, but it's also really important to think about what San Diego is and what San Diego means to the United States. San Diego as a county is 1% of the entire population in the United States. So when you do things in San Diego, you do them in America in a scale that you can't do in any other metropolitan region. The second thing that makes us unique is this high correlation of civilian and military assets. And I think my colleague Mark would agree with me, there's not a hard boundary between a lot of what we do. The very infusion of our society means that folks are moving back and forth. And we certainly know that outside actors are always looking for a way to find a permissible corridor that they can get in. San Diego, because of the very unique concentration of private, public and military sector assets, has something that's really unique and certainly that plays forward."

He continued: "Mission Valley is a living laboratory, which is a small city inside of San Diego with one landlord focused on new knowledge diffusion, how do we bring together public and private sector partners in pre-competitive opportunities to show things at scale. So the opportunity in Mission Valley is to take a good idea and to show how it could actually impact what goes on in a stadium, what goes on in a hotel, what goes on in a residential housing area. All of those things being done and fueled with the enthusiasm and the innovation that you have from our Aztec students, the faculty and the partners that we bring together."

Easterly concluded by thanking the panelists.

"I know I'm quite energized," she said. "I hope our listeners are ready to join the fight with us." She invited the program's listeners to visit sdccoe.org for additional information, free resources and the opportunity to register for a complimentary cybersecurity awareness program available to all small businesses with less than 100 employees in our region.

The next San Diego Business Journal Cyber Trends panel discussion is planned for the fall. ■