

SDBJ, CCOE Survey Cyber Landscape for '22 and '23

CYBERSECURITY: Government Urges 'Shields Up,' Local Experts Here to Help

■ BY BRAD GRAVES

Intrigue, heroes and shadowy villains. Software with titles like BlackEnergy and Industroyer.

At times, the quarterly panel discussion in the **San Diego Business Journal's** Cyber Trends 2022 series had a film noir feel, with tales of criminals and their counterparts (the ethical hackers) battling over the servers of U.S. public agencies, or operating in the background of a war in a distant part of Europe.

It was the fourth quarterly discussion in the video series, held in early November, with representatives of private industry, government and academia engaged in conversation about all things cybersecurity.

As usual, it was convened by **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.

Lisa Easterly, president and CEO of CCOE, was moderator for the video discussion. She kicked off the event with a welcome and a few reminders about what is at stake.

"Cybersecurity is now everyone's business," Easterly said. "The **FBI** reports a 300% increase in cyber-crimes across all industries since the pandemic began. With the average cost of a data breach climbing over \$4 million, more than half of these costly attacks are aimed at small

and medium-sized businesses, and that is our region's economic engine. 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 77,000 openings here in California—and it really becomes mission critical to integrate cybersecurity into our daily business practices."

There is optimism hidden in those numbers—and it is more than the availability of jobs. It's an economic impact larger than the biggest blockbuster events San Diego might host.

"The good news is 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**," Easterly continued. "This cluster now accounts for more than 24,000 jobs and has a total economic impact of \$3.5 billion annually. That's equal to hosting nine Super Bowls or 23 Comic-Cons. This collaborative ecosystem is developing new technology defenses and cyber warriors to combat this ever-evolving threat landscape."

The Fall 2022 discussion, Easterly said, taps into the robust expertise of the panel, looks back at the cyber trends of the year, evaluates the current threat landscape, takes lessons from the trenches and looks at new innovation.

With that, Easterly welcomed the panel.

Seeing the Issue From All Sides

The panelists included **Tony Anscombe**,

chief security evangelist for **ESET**, a cybersecurity company. "We've been around for 30 years and our North American headquarters are in San Diego." The building with the ESET sign is a downtown landmark, "which is always pleasing to see when I land at the San Diego airport," Anscombe said.

Next, **Joseph Oregon** introduced himself as the chief of cybersecurity for **CISA**—that is, the federal **Cybersecurity and Infrastructure Security Agency**. He is in charge of the area federal officials call Region 9, which incorporates the states of California, Arizona, Nevada, Hawaii and U.S. territories far in the western Pacific Ocean.

"And you wear a cape. We know. We just can't see it on video," Easterly said with a laugh.

And he carries the flag, Oregon said good-naturedly.

Chris Simpson, director of the **National University Center for Cybersecurity**, introduced himself next. "We're headquartered here in sunny San Diego, and we are an **NSA** Center of Academic Excellence in cyber defense education," he said. "And we have bachelor's, master's and now a doctoral degree in cybersecurity."

Hackers Eye Schools

With introductions accomplished, Easterly offered a prospect of San Diego from a hacker's point of view. The community "is home to a vibrant

innovation economy, the tourism industry and the largest concentration of military assets in the nation, which creates a large bullseye for bad actors," she said. "So Joe, what is the Cybersecurity and Infrastructure Security Agency—or **CISA**—seeing as the key threats impacting our region that all organizations should have on the radar?"

"There are so many things going on as it pertains to threats right now," Oregon said. "At **CISA**, we're observing a significant uptick and attacks against critical infrastructure across the board, but specifically as we look at K-12 and our education system just recently, we observed several attacks against our education system here in the state of California. In itself, that issue has been pretty significant."

He said **CISA** Director **Jen Easterly** has instructed regional personnel to focus additional resources and increase outreach efforts to K-12 partners within the region and throughout the United States.

"So we've been working very closely with our state partners at the California Governor's **Office of Emergency Services** and the **California Cybersecurity and Integration Center**, along with fusion centers and a lot of private sector partners such as CCOE and others to coordinate our support for our K-12 partners."

➔ *Cybersecurity page 42*

MODERATOR



LISA EASTERLY

Lisa Easterly is president and CEO of the **Cyber Center of Excellence**, 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, she served as CCOE's founding chief operating officer. In this role, she developed the organization's infrastructure and operations, creating substantive programs to grow the organization. Easterly has served in various roles at nonprofits working to elevate the region's tech ecosystem. She was a founding board member of **CleanTech San Diego** and Chair of the **Education & Outreach Committee**—developing the initial branding, outreach strategy and marketing collateral to launch the organization. Additionally, she served as vice president of marketing for the **San Diego Regional Economic Development Corporation**.



TONY ANSCOMBE

With over 20 years of security industry experience, **Tony Anscombe** is an established author, blogger and speaker on the current threat landscape, security technologies and products, data protection, privacy and trust and internet safety. His speaking portfolio includes industry conferences **RSA**, **Black Hat**, **VB**, **CTIA**, **MEF**, **Gartner Risk and Security Summit** and the **Child Internet Safety Summit**.

THE PANELISTS



JOSEPH OREGÓN

Joseph Oregon is the chief of cybersecurity for the **Cybersecurity and Infrastructure Security Agency (CISA)** Region 9. His area of responsibility incorporates the states of **CA**, **NV**, **AZ**, **HI** and the U.S. territories of **American Samoa**, **Guam**, **Saipan (CNMI)**. Oregon supports the **Department of Homeland Security (DHS)** mission of strengthening the security and resilience of the nation's critical infrastructure. His program coordinates cyber preparedness, risk mitigation, and incident response and coordination, and provides cybersecurity resources, including assessments and training, to the nation's 16 critical infrastructure sectors, state, local, tribal, territorial government entities and private sector stakeholders.



CHRIS SIMPSON

Chris Simpson is the director of the **National University Center for Cybersecurity** and is the academic program director for the master of science in cybersecurity program at **National University**. He has developed innovative curricula and labs in ethical hacking, penetration testing and incident response. He retired from the **U.S. Navy** in October 2009 after 27 years of service. He has extensive experience as an information assurance manager, including a tour as the information assurance manager (**IAM**) for the **Commander, Combined Forces Command Afghanistan**. He holds a bachelor of sciences degree in computer and information science (**CIS**) from the **University of Maryland** and a master of science degree in information security and assurance from **George Mason University**. He is currently a doctoral student at **Dakota State University**.

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



Cybersecurity

➔ from page 40

With that, Easterly noted there has been a 75% increase in cyberattacks on education since the pandemic, according to Check Point Security. “The education industry not only has to deal with many of the threats that Joe mentioned; they also have to prepare the workforce to combat these risks across all industries.” Turning to Chris Simpson, she asked about the lessons National University has learned about working with industry to best prepare the workforce to deal with such evolving threats.

“Universities face many of the same threats as industry,” Simpson said. “Our workforce and our students are both local and remote. So we have to deal with protecting those assets. And additionally, universities are targets for attackers because of the wealth of information in the university systems: financial information, private information and then research information. So we have to make sure we protect that information. And then while facing these threats, we are also preparing the future workforce to fight against these threats. And as you noted, these threats are evolving, so we have to keep up our curriculum to make sure the students are really prepared to deal with that. In our program, we’ve implemented a significant amount of hands-on training that simulates real world environments including hands-on labs.

“Additionally, we have a capstone project where students go out and support an organization to increase their security. So this not only gives students hands-on experience working with a real company, but it offers a small business—or even a large business—an opportunity to increase their security. And for the small businesses, in many cases, they can’t afford that. So it’s free work for them.

“And I recently saw a talk from another university where the university had a shortage of their security operations center staff. So they went to their academic team and they started having their students work in their security operations center, after some training. Not only did that enhance their security; it also helped the students gain that real-world experience.”

“Absolutely,” said Easterly. “We really like to see the collaboration between industry, academia and government to tackle the threats and also look at where the innovations and solutions lie.”

International Intrigue: Wipers and More

She then turned her attention to Anscombe.

“So we’ve seen this year that the war on Ukraine has dramatically impacted the cyber risk landscape. And ESET was actually one of the first to detect malicious malware campaigns used in numerous attacks against the country and its supporters. So Tony, can you share the highlights of ESET’s research activities from this conflict as well as the lessons learned and best practices to strengthen cybersecurity posture and mitigate cyber threats that are applicable to all businesses?”

“The posture and landscape have certainly changed this year with probably what is the first, I would say, understandably visible cyber warfare that any of us have ever seen,” Anscombe said. “I’m sure it’s been going on for a number of years behind the scenes, but this one is very

much in the news.

“To start with, we saw critical infrastructure attacks back in 2015 and 2016 with BlackEnergy and Industroyer [malware] with blackouts in Ukraine. And of course that’s post the annexation of the Crimea area. But what was interesting of that, [in] 2016, we detected what was then the first piece of industrial control system malware. Now, industrial control systems are what I define as a black box. You know

“

‘The posture and landscape have certainly changed this year with probably what is the first, I would say, understandably visible cyber warfare that any of us have ever seen. I’m sure it’s been going on for a number of years behind the scenes, but this one is very much in the news.’

TONY ANSCOMBE

their box is running firmware, and they’re running some sort of process Malware written for an industrial control system is incredibly complex and it’s incredibly sophisticated. The attacker needs to understand how the box runs, the protocols running on the box, how the box is deployed somewhere, and how it’s being used. So we learned a lot back in 2016.

“Well, with the conflict starting in February/March time, we detected a number of data wipers. Now, we all tend to think about ransomware and encrypting data. Data wipers are exactly as they sound They’re malicious and they destroy data and they’re used for disruptive purposes. And there’s a number, a series of data wipers from the beginning of this year up to the conflict and beyond the start of the conflict. And we detected one being deployed the night before ground forces went into Ukraine, and it was deployed around 5 p.m. local time in Ukraine.

“We called this Hermetic Wiper because of the signature in this particular malware. And in fact, if you want to read further information on that, you can either come to WeLiveSecurity.com, or CISA has some great research. And we’re attributed with our research through CISA as well. I’d like to thank Joe for the partnership we have with CISA on sharing that type of information.

“But then if we fast-forward into April, we saw a new variant of Industroyer, [named] Industroyer2. So, [it was] a new variant of this industrial control system malware. Now here it has evolved as you’d expect over the course of five or six years. And the good news is this was an attack successfully stopped by CERT [the emergency response team] Ukraine and by ESET in joint cooperation together. We’re the guys that have the deep understanding of this particular piece of malware, and they had some intelligence that there may be an attack against their critical infrastructure.

“So this is the good news, but it’s interesting to see how this industrial control system malware was used against the power grid in Ukraine. And I think we are all seeing how significant power grids are in a conflict zone because now they’ve taken to destroying [the grid] with other

forces as opposed to cyber forces. But with that, they also deployed a number of data wipers. So think of the confusion in a substation or within the power company where not only are your industrial control systems being attacked, causing instability in your grid, but if data wipers are trying to destroy admin stations and other workstations as well. It causes disruption. And of course, it destroys forensic evidence for people like us to see how the attack took place; what could be learned from it and how we could protect against it in the future.

“But fortunately, like I say in this instance, we got to it before it happened.”

Domestic Lessons, Small Business Help

Anscombe said this is an important lesson for U.S. utilities, adding that CISA has great advice for people who run the nation’s critical infrastructure.

“I keep looking around at all these small water utility companies in the U.S. There are 54,000 of them! It’s such a massive task. The importance is take cybersecurity seriously. Very seriously. You are a target without question, at some stage, whether that’s somebody trying to monetize or whether that’s somebody trying to destroy things. Make sure you’re updating systems and make sure that you’re looking at the traffic that’s happening on your network. So make sure you’re using an XDR system and actually looking at traffic, patterns, et cetera. And if you don’t have the expertise in-house—because we know there’s a mass shortage, you bring in experts. We’re happy to talk to you. The CISA guys are happy to talk to you. There’s a lot of expert cybersecurity companies around and it’s got to be something companies budget for in order to protect the critical infrastructure we all rely on.”

At this point, Joseph Oregon joined the conversation.

“I’d be remiss if I didn’t take the op-

“

‘CISA does have a cisa.gov ‘Shields Up’ website. And we brought this to our constituents and to our stakeholders across the United States and for every organization, large or small, because we understand the importance of being prepared to respond to disruptive cyber incidences.’

JOSEPH OREGÓN

portunity to piggyback on Tony’s comments and fantastic advice across the board. And I would also encourage to our partners that CISA does have a cisa.gov “Shields Up” website. And we brought this to our constituents and to our stakeholders across the United States and for every organization, large or small, because we understand the importance of being prepared to respond to disruptive cyber incidences.

“So I would definitely encourage visiting cisa.gov Shields Up and to utilize and leverage some of those resources that we provide out to all all partners for free,” for free,” Oregon said with a nod.

Easterly noted that CISA is one of her favorite resources, especially the

small business guides.

“So many small businesses don’t even know where to start,” she said. “And because we have such a shortage of cyber professionals, they’re so stretched as well.”

At that point she asked Chris Simpson about suggestions for companies—including resource-stretched small businesses—to attract, retain and upscale cyber talent to thwart the threats that the other panelists spoke about.

Benefiting Students and Companies

“First,” Simpson said, “to piggyback on Tony’s comments, I would suggest organizations reach out to academia. Not only do you have faculty conducting research and they can support organizations, but also their student base or doctoral students and graduate students too

“So for some of the smaller organizations, there are a couple things I would suggest. First of all, I would encourage them to take advantage of the local programs in the area. Here in San Diego, we have CyberHire and they connect universities—they vet their programs first—and then they connect students with potential employers. They have some resources to help offset some of the costs for those students participating. So not only do employers get additional work at maybe a lower cost, the students are getting their experience in that organization.”

If it’s a good fit, a company may end up hiring the university students, he said. All in all, he said, it is “a great, great opportunity for small businesses.”

“And I would also just reiterate, take advantage of universities here in San Diego. Our capstone students, they’ll come in and in many cases the small business, they could not otherwise afford some type of security assessment. Our students will get them started. We use the CISA website. We use a lot of the NIST resources and checklists. And we have our students go through those and they at least get those organizations up to a base level. We particularly work with a fair amount of small doctors’, dentists’ offices, some DoD contractors, making sure they’re getting up to speed.

“For some of the larger organizations, I would encourage them to support their local K through community college communities. So here in Southern California, we have the SoCal Cyber Cup. It’s a middle school, high school and community college cyber competition that helps students learn about STEM and encourages them to consider cybersecurity a career field. Last year we had 670 or so students participate in the five [participating] counties here in Southern California. ...

“We always need mentors to help the teams out,” he continued. “And our mentors always have a great time helping the students. And then also financial support, donations to help make sure we keep the competition going. And students, they get a real environment where they have to defend off some attacks and things like that. So it’s a great experience for all participants in the SoCal Cyber Cup.”

Sharing Information: CISA Wants You

The human element can hurt and help a cybersecurity posture, Lisa Easterly observed.

Local impact— Global influence

With headquarters in Little Italy, ESET North America is a local presence—and a global leader in cybersecurity.

For 30+ years, we've protected organizations and governments worldwide from the latest cyberthreats.

Our multilayered approach to security and our investment in research—with hundreds of researchers in 13 R&D centers around the globe—sets us apart from other digital security companies.

ESET is trusted by some of the biggest names in business, technology and education. As part of Google's App Defense Alliance, ESET helps protect the Google Play Store for millions of users.

But here in San Diego, we're just another local business. We're proud to support local nonprofits, charities, schools and foundations.

And we're honored to be part of this community.

Go to www.eset.com to learn more.



Digital Security
Progress. Protected.

Cybersecurity

➔ from page 42

“We’ve definitely seen that, through the last year, people are both the greatest weak link in cybersecurity with 95% of cyber breaches resulting from human error,” she said. “But the good news is they’re also the strongest link in that they’re our first line of defense. And so just basic preparation and education of your employees and working with your local education institutions to do so is absolutely critical. And I know ESET has a phenomenal program that we’ve been able to tap here at Cyber Center of Excellence to help small businesses just become more cyber aware and not to click on the scary link. So I think it’s been a great discussion about the lessons businesses can learn from the cybersecurity trenches, but let’s turn the tables a bit.”

“This is my favorite part,” she continued. “Joe, if you can speak to some of those top cybersecurity challenges like ransomware, ‘Joe, if you can speak to some of those top cybersecurity challenges like ransomware, infrastructure challenges faced by U.S. Department of Homeland Security, and then how can industry help?’”

“Excellent question,” Oregón said. “You hit on a key topic there when it comes to our folks, our people. Information sharing amongst ourselves as a society, from our local counties and federal level down to the private sector partners.

“Sharing information such as indicators of compromise is huge,” he said. “In order for CISA to understand the unique challenges we face as a nation, it is critical that we hear from our partners. So information sharing is crucial, and we work hard to establish trust, confidence with American people, with American businesses, in hopes that we can understand the dynamic together and better defend our country against these adversaries. So as we look at some of the main challenges there, I would rather start kind of small and tackle some of those old paradigms with sharing information between different agencies as well as private sector and public alike.”

Easterly then asked about resources for an organization that suffers a breach; “what resource do you point them to as a first stop?”

“So ourselves at CISA, as well as our partners at FBI, Homeland Security Investigation down to the fusion centers are all set up to ingest information from partners,” Oregón said.

“I would encourage partners to really take a look in your local area for your fusion center. Fusion centers have been set up—and we’re very fortunate here in San Diego to have the San Diego Law Enforcement Coordination Center—but fusion centers are set up to triage information at the local level, and triage that all the way up to the federal level for our visibility. And in turn, we use that as a means for us to disseminate information back down to the local level. So I would highly encourage our partners to definitely leverage fusion centers. And we’re lucky in the state of California: we have six fusion centers overall for the state, with the Cal-CSIC, the California Cybersecurity Integration Center, at the helm”

That Urge to Click on a Link

“Fabulous,” Easterly said. “And we’re quite excited here in San Diego. On our last panel, we had the San Diego Regional Cyber Lab, which is launching before the end of this year, opening their doors to support infrastructure partners, small businesses, and to provide our academic

partners opportunities to have real hands-on experience. And again, to Joe’s point, it’s about sharing information. “The good news here is that cybersecurity really is not all doom and gloom. I know we have a tendency to focus on the cybersecurity threat landscape, but as threats are evolving so are the resources and tools available to increase cybersecurity awareness and preparedness. Tony, can you speak to some of those new innovations and resources available to organizations, big and small?”

“I certainly can,” Anscombe said, “but let me add something: congratulations to CISA, Department of Homeland Security, Department of Justice and FBI, et cetera. It’s not all doom and gloom! We’ve just seen [convictions of] two cyber criminals in the U.S.: one in prison for 20 years, and one in prison for 25 years. One a prolific business email compromise and romance scammer, and the other one, an affiliate of the network again. So I’d just like to pass on my congratulations to law enforcement actually getting justice and bringing some of these people to account for their actions.



‘Take advantage of your local academic institutions here in San Diego. You’ve got not only us at National University, you’ve got Cal State San Marcos, they’re another center of academic excellence. University of San Diego, same thing. Palomar College, San Diego State. So there’s just a wealth of knowledge and experience here in this area to support small and large businesses.’

CHRIS SIMPSON

“But coming back to your question about cybersecurity training. This is, as you said, 95% of cyber incidents are of human behavior. And you hear different stats from different places, but it’s always around that 85% to 95% range.

“And unfortunately, we have a propensity to click. You know: something lands in our inbox and it may be timely, or it just may be interesting, or it may be well crafted. You know, if you’re expecting a DHL delivery and a DHL-looking email lands in your inbox, and we’re on the run, then we may actually be tempted to click on it. And cyber insurance has certainly played a big role in most employers now have cybersecurity awareness training on an annual basis. You know: that course that you sit down and take for 30 minutes or 45 minutes. And as you correctly pointed out, Lisa, we can provide ESET cybersecurity awareness training.

Giving ‘the Mandatory Course’ Some Spark

“But I’d say here that once a year isn’t enough. It is just not frequent enough. We sit down [and] it’s that mandatory course you need to take. And I think this should be a short refresh every three months. And somehow that refresh should be looking at the campaigns that cyber criminals are running.

“For example, in the four months running from May through the end of August, we saw a sixfold increase in phishing campaigns

using shipping email attempts,” he said. These are messages purporting to be from DHL or the U.S. Postal Service, or something similar.

“Now, cyber criminals run these as business campaigns in the same way that we run campaigns to sell products or promote services or to push something out. Cyber criminals are doing exactly the same. So if we ran training on a frequent basis, every three months, I think it will become more focused, more real time.

“I’d urge all businesses to do this on a frequent basis, even if it doesn’t mean full training, but sending around examples to employees. You know: ‘This is the latest phishing tactics that we are seeing, be on the lookout for these ones. It might appear in text, it might appear in email.’ Give people good warnings. It has just been Cybersecurity Awareness Month, last month in October. [It is] an important month for all businesses to reflect and to take stock of what they’re doing. But I look back 10 years ago, and 10 years ago the topic was phishing, and this year it’s phishing, along with a couple of other topics in there. This is something we don’t seem to be able to fix as an industry or as society.

“So I kind of want to put it out there. And I urge educators at the younger ages, let’s try and get to kids before they start clicking, and just make them understand that if something turns out of context in email or unexpected, it’s not something you’ve asked for, a password reset or whatever it might be, don’t click it. Just don’t click it. And if we can get our kids doing it now, maybe in 10 years’ time, the phishing will be removed from cybersecurity awareness month. And wouldn’t that be a unique happening?”

“Absolutely,” said Easterly. “I can’t tell you how many times I tell my kids not to click on suspicious links. Think before you click, that has to be every family’s motto.

“And it was very interesting to me,” she went on, talking about the sources of such texts and emails. “We recently had a program with the FBI here in the region that, to Tony’s point, highlighted how these bad actors from nation states operate almost like corporations. They’re an employee. They clock in with a timecard. There have HR and IT departments. And if you click on that email, you are unfortunately providing an opening not only to potentially your employer, your businesses, but also to your homes and your families. So great advice.”

Concluding Thoughts

At this point, Easterly asked for final thoughts from the group: ideas “from the trenches that could potentially help our audience navigate the cyber threats we’ve seen this year.”

“Also,” she asked, “what you’re seeing on the horizon for 2023?”

“To reiterate, take advantage of your local academic institutions here in San Diego,” said Chris Simpson. “You’ve got not only us at National University, you’ve got Cal State San Marcos, they’re another center of academic excellence. University of San Diego, same thing. Palomar College, San Diego State. So there’s just a wealth of knowledge and experience here in this area to support small and large businesses and for businesses.

“I would also encourage you to look at your job requisitions,” he added. “I’ve noticed there’s a lot of job requisitions for entry level [positions] that, you know, want 35 years of Amazon experience. I know I’m exaggerating a little, but, entry level folks, they’re not going to have all that experience. But ask what they’ve done in their institutions. Most of the universities, we give students some hands-on training now with various labs on different platforms. So take

advantage of that and then work them into your system rather than trying to look for that specific ... they call them a unicorn.

“There’s a ton of talent here nationwide and especially here in the San Diego area. So take advantage of your local universities and training centers.”

Easterly then asked Oregón for a final thought.

“I would probably hark back to an old saying: It’s not if, it’s when. So as we kind of take a look at incidences, I think it’s important to pull away that encouragement there. And that’s for our partners to reach out and make contact with your local CISA rep, with your local FBI, fusion centers or state cyber components. [By making contact] well in advance of an incident, it can provide a tremendous amount of resource as well as add value to any existing incident response plan [by] just understanding who’s who and your backyard well in advance.

“And so thank you, Lisa, for that opportunity to speak to our guests today,” he said.

“Absolutely,” Easterly said. And Tony, we’ll have you take us home.”

“Obviously cyber threats are growing and I think we all recognize that,” Anscombe said. “As we head towards the end of the year, it’s a great time, I think, for businesses to take stock, look at and dust off their cyber resilience plans. Do a cybersecurity audit and take some of these things seriously and actually look to see what you’re doing.

“One thing I would say: I recently presented in Australia at a conference and three people in the audience admitted to having paid the ransomware demands, which, unfortunately, is not uncommon. But interestingly, all three—and they were from small businesses—said the same thing: we paid because we didn’t have a backup. So I’d urge anybody listening to this webcast today to make sure you understand that you are backing up, that you are disconnecting your backup and that you know how to restore it, most importantly. And obviously you need good cybersecurity and all those other good things as well—I definitely say that as ESET—but I’m just saying, you know, if you’re paying ransom because of a backup, it’s just such an easy thing to have fixed right out of the gate. Take the money out of cybercrime and hopefully we get rid of some of these cyber criminals.”

“Oh, that’s absolutely great advice,” Easterly said. “And as one of our board members always says, an ounce of prevention [is worth a pound of cure] having to restore and recover. And particularly now with what’s happening in the insurance markets where nation state attacks are seen as acts of war now. And so folks can’t just rely necessarily even on cyber insurance. And so employee training, preparation, working locally and having connectivity are really kind of key to helping prepare for, as Joe says, the When and not the If.

“So we absolutely love the conversation today. Thank you so much, Tony, Joe, Chris, for these really insightful thoughts for our audience. We invite our listeners to visit CCOE’s website, at coe.org, as well as CISA, National University and ESET for lots of additional information and free resources. We also currently have openings for the cybersecurity awareness program I mentioned, which is free to all small businesses here in the San Diego region. So check that out.

“And then we also just thank you for joining us for our four panels this year in special reports.

Easterly thanked her panelists, and said a Cybersecurity Trends 2023 series will be kicking off in the new year.

“Stay tuned,” she said. ■



Help Protect The World's Information Systems.

The need for cybersecurity professionals continues to grow, and National University's cybersecurity programs are meeting the demand. These workforce-ready online learning opportunities include hands-on learning experiences that are crucial to success in the field.

National University has been designated by the National Security Agency as a Center of Academic Excellence in Cyber Defense (CAE-CD).

Why Choose Cybersecurity at NU

- 4-week courses designed for adult learners
- Faculty are industry leaders
- Seamlessly transfer community college credits
- Experiential learning opportunities, hands-on labs, and competitions
- Career and job placement support through CyberHire partnership
- Free tutoring, mentoring, and wellness counseling
- Millions in scholarships



Learn more at
NU.edu

