SDBJ.COM

SAN DIEGO BUSINESS JOURNAL

Vol. 43, No. 9 — THE COMMUNITY OF BUSINESS™ — February 28 – March 6, 2022 • $5.00

Photo courtesy of Town & Country Resort

The Town & Country Resort's $100 million makeover honors its past.

Whimsical Messages Help Draw Curious to Hotel Row Property

TOURISM: Historic Town & Country Resort Gets $100M Makeover

■ By RAY HUARD

Before it underwent a $100 million renovation, the Town & Country hotel in Mission Valley was attracting notices that did little to attract guests.

"The hotel was not in the best of shape and social media wasn't exactly kind to us," said April Shute, who has been vice president and managing director of Town & Country since January 2017.

"We thought, well, let's try to change what people were talking about," Shute said. "We decided let's just do stupid signs every week and see what happens."

One of the first postings on the hotel marque read "Welcome archery tournament, free ear piercings."

"People stopped to get their ears pierced," Shute said. The hotel didn't do ear piercing,

➡ *Town & Country page 10*

Experts Offer Solutions to Cyber Threats

TECHNOLOGY: SDBJ, CCOE Host a Panel Discussion

■ By BRAD GRAVES

Anyone doing business in 2022 needs a certain talent.

Call it internet savvy.

It's something that mixes technical know-how, street smarts and a lot of heart.

In 2022, every business — from the largest tech conglomerate to the smallest startup — is a digital business. As such, it needs to care about cybersecurity.

Cybersecurity is now everyone's business, said **Lisa Easterly**, president and CEO of the **Cyber Center of Excellence** (CCOE) in San Diego.

CCOE joined the **San Diego Business Journal** this month for the first installment of a four-part series called Cyber Trends 2022. The series will culminate with a cybersecurity stewardship awards program in the fall.

A video of the first cyber panel discussion is available on the San Diego Business Journal website at www.sdbj.com. It is also posted on YouTube at https://www.youtube.com/watch?v=7PoiNOanGZw

Lisa Easterly
CEO
Cyber Center of Excellence

The discussion brought together three panelists with hands-on experience and deep insight into the cybersecurity landscape. They are **Sai Huda**, CEO of **CyberCatch**; **Andre Polakoff**, founder and chief technology officer of **SearchBug Inc.**; and **Miguel Sampo**,

➡ *Cybersecurity page 36*

Banner Year for Seismic

SOFTWARE: Robust Revenue Tops $280M

■ By JEFF CLEMETSON

Earlier this month, **Seismic** announced another banner year for the company, with revenues in excess of $280 million for its fiscal year ending Jan. 31, 2022.

Doug Winter
CEO
Seismic

Along with a 50% increase in annual revenue run rate year over year and its best quarter in company history, on Feb. 3 Seismic reported robust growth across its customer base, people and international footprint, including:

➡ *Seismic page 10*

Building Out Carlsbad's Industrial Base

REAL ESTATE: Techbilt Launches New Projects

■ By RAY HUARD

The **Techbilt Companies**, a family-owned commercial real estate and housing developer based in Loma Portal, is starting a series of construction projects that will cover much of the remaining industrial land in Carlsbad.

"There are a few places here and there, but there's not very much left," said **Ted Tchang**, president and CEO of Techbilt.

"Like anything, real estate is cyclical. Right now, it's as strong as I've ever seen it in my career," Tchang said. "As the Carlsbad market has matured, we've seen the average

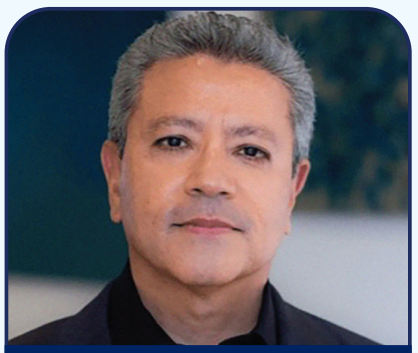
➡ *Techbilt page 43*

MODERATOR

LISA EASTERLY

Lisa Easterly became president and CEO of the San Diego Cyber Center of Excellence in 2021 after serving as chief operating officer and strategic adviser since 2014. The organization promotes regional planning, programming and best practices in cybersecurity, bringing together academia, industry and government, including federal law enforcement and the military. 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.

THE PANELISTS



SAI HUDA

Sai Huda is the founder, chairman and CEO of San Diego-based CyberCatch. He is a globally recognized risk and cybersecurity expert and the author of the best-selling book, "Next Level Cybersecurity" and a frequent keynote speaker at industry conferences. He was previously the founder and CEO of Compliance Coach, an innovative compliance risk management software as a service (SaaS) company, which was acquired by FIS, a Fortune 500 company. He also led the inaugural training program for Consumer Financial Protection Bureau (CFPB) examiners. He serves as an advisory board member for the Cyber Center of Excellence (CCOE) and the CIO Strategy Council.

ANDRE POLAKOFF

Andre Polakoff is an information technology services professional with 25 years of experience in implementing enterprise systems for human resources. He has developed innovative technology solutions that increased the efficiency of business processes and achieved multimillion-dollar savings for prominent U.S. and global companies. He is also founder and CTO of SearchBug, an online B2B company in Carlsbad that he started while working at Rockefeller University in 1995. Originally called search-it-all.com and renamed in 2000, SearchBug helps businesses and consumers find the contact information they need. Polakoff has a Ph.D. in molecular biology.

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 1*

senior director of **RiskRecon, a Mastercard Company**.

A Look Ahead

The four spoke about the biggest cybersecurity risks and challenges for the coming year. It's going to be a big year, they said.

One of their main points was that small and medium-sized businesses will face challenges just like their bigger counterparts.

The good news is that there are steps that every business can take to build cyber hygiene.

On top of that, technology can lend a hand in the cybersecurity fight, specifically with new forms of automation.

Not to be overlooked are supply chain relationships between companies. Bad actors seem to find ways to exploit those relationships to make money.

Awareness of that fact is a good first step in fighting the bad guys.

The Cybersecurity Landscape

Easterly kicked off the conversation by noting that the **FBI** is reporting a 300% increase in cybercrimes across all industries during the two years of the pandemic. By now, the average cost of a data breach has climbed to more than $4 million.

More than half of the attacks are aimed at small and medium sized businesses — which are the engine of many regional economies, including San Diego's.

This is all happening during a time when companies, even governments, are shorthanded. There is a global shortage of cyber professionals to thwart these attacks. "It becomes mission critical to address the systemic risk," Easterly said.

The good news is that San Diego is leading the charge with more than 870 cyber firms, as well as the **U.S. Navy**'s **Naval Information Warfare Systems Command**.

San Diego's cybersecurity cluster now accounts for more than 24,000 jobs and has a total economic impact of $3.5 billion. The figure is equal to hosting nine Super Bowls or 23 Comic-Cons annually.

This collaborative ecosystem is developing new technologies, defenses and cyber warriors to go up against this ever-evolving threat landscape.

In the News

After introducing the panelists, Easterly spoke of the large scale cyberattacks that have taken place since the beginning of the coronavirus pandemic. Colonial Pipeline, Kaseya and Solar Winds made headlines in the mainstream media.

The news comes during an era when hostilities between nations often include cyberattacks. We in the United States have the potential to feel that, "not directly but indirectly," said Sai Huda.

"I'll point to what happened five years ago with NotPetya," he said. "If anybody remembers, it was one of the worst attacks faced globally. And over $10 billion in losses happened from that ransomware. And what happened there was a Russian group, backed by the government of Russia, went after an accounting software company in Ukraine because they had a lot of government customers in Ukraine. And what they wanted to do was infect that company with ransomware, which they did in its software update process."

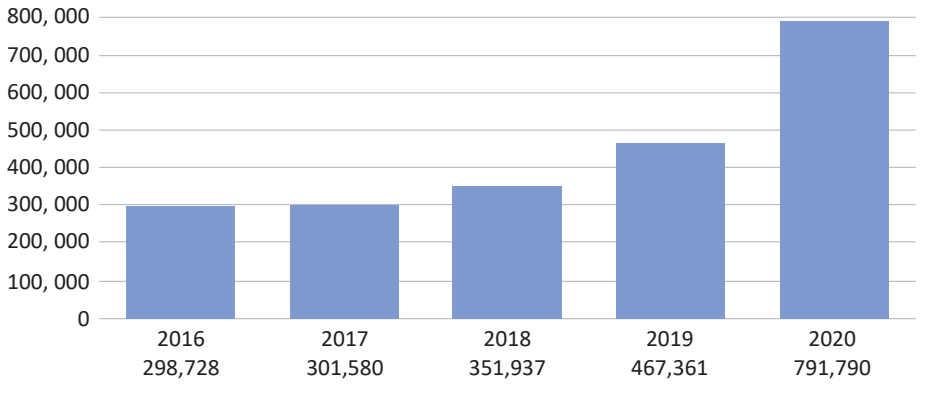
The software was able to encrypt the boot of a computer irreversibly. The goal was to stop operations, wipe out data and cause damage.

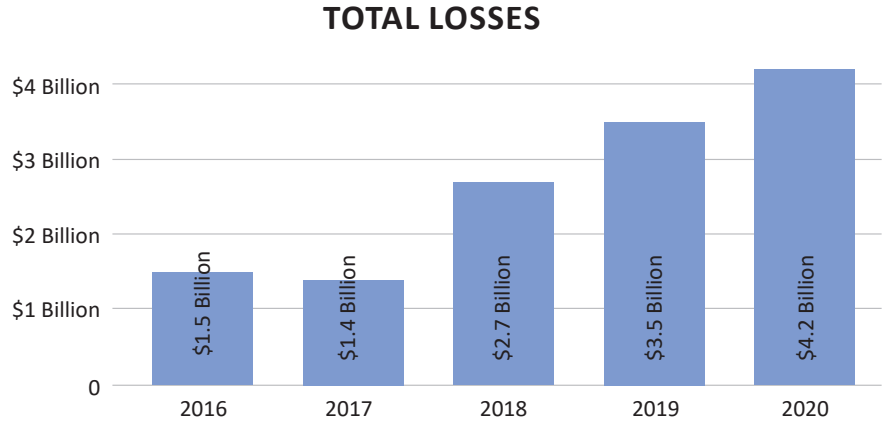
An unintended consequence of that, Huda said, was that thousands of companies throughout the world, especially in the United States, were impacted because they were also customers of that accounting software company. "And those folks suffered significant damages from not being able to recover from the ransomware for days, weeks and months."

As of Feb. 14, the day of the panel discussion, U.S. government agencies were telling organizations to beware of what's going on with the hostilities between Russia and Ukraine, Huda said. There may be ripple effects, he said.

"Every single organization in the United States must take this seriously," Huda said.

Complaints to the FBI's Internet Crime Complaint Center (IC3)





Source: FBT

Woes With Old Software

Hackers do their work by taking advantage of vulnerabilities in certain software, which brought Huda to a point about a second threat. Criminal gangs and governments, he said, are exploiting older and "lower score" vulnerabilities to software.

Software vulnerabilities are assigned a score by the U.S. government's National Vulnerability Database. People pay most attention to the worst of the vulnerabilities, with scores of 9 or 10, when it comes time to patch software. Many organizations with limited resources don't get around to patching software with lower-score vulnerabilities.

"I predict, unfortunately, that 2022 will be a year where there'll be a lot more of those exploits," Huda said.

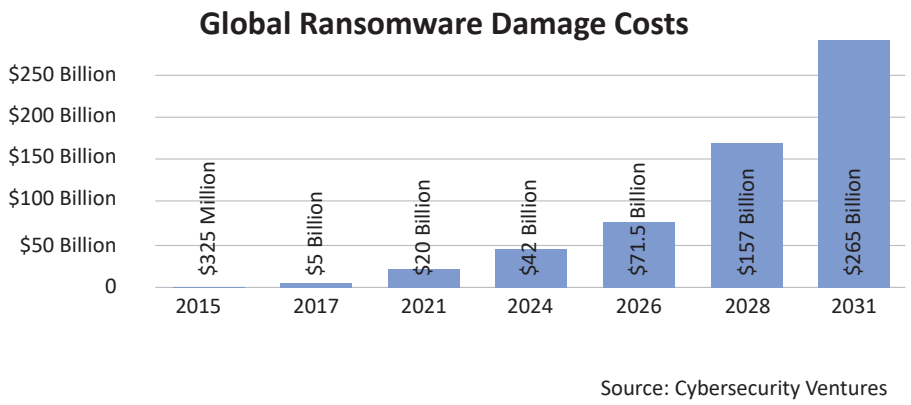
Huda also spoke about CyberCatch's own, recently published research. The company examined the public-facing parts of the internet at 21,850 small and mid-sized businesses in the United States and Canada, and found an alarming number of businesses vulnerable to hacker techniques such as "Spoofing," "Clickjacking" and "Sniffing."

'We've Seen It All'

Easterly then turned to Andre Polakoff and asked about possible threats to small and medium-sized businesses — observing that small business owners have plenty of other challenges, such as digital transformation and economic uncertainty. Why, she continued, are small businesses being targeted?

Polakoff noted that hackers are interested in stealing credit card information and passwords. Such information can be sold on the black market. Password information is especially valuable because people frequently use the same passwords on multiple accounts, he said.

Small businesses are attractive targets, he said, because they have minimal resources.



Source: Cybersecurity Ventures

They may outsource website development and not emphasize security in their website design. They might leave password or credit card information in plain text — which is easier for a would-be hacker to use once it is in hand.

"If your business is providing some valuable service information, you will be a target," he also said. His business deals in consumer data that people in the outside world would like to get for free.

Hackers using stolen credit cards can cause multiple headaches for a business. Card processors can charge fees, "and you can even be banned by a processor."

Polakoff recalled that 15 years ago, one big financial services company "called us one day and said because of the high chargeback rates, your business account has been closed and you can no longer accept credit cards."

It was very sudden, he recalled. "And there was no advance notice, [no way] we could negotiate. And all of a sudden, because of the high chargebacks we got, we were out of business, couldn't collect any revenue until we built a new integration with another provider."

Another common way hackers can access a website is through a technique called SQL injection.

"Basically what they do, they manipulate query strings, or they put something in the forms, and they do it in an automated way to trick your database that you're not only searching for a customer order — but also show me additional information, how your database is structured. And so once they find what database you use … then they try to manipulate it." A hacker can attempt to get administrative access, or to get services for free.

The password reset function of a website can be "tricky" feature and a potential problem, he said.

"We 've seen it all," Polakoff said with a weary laugh.

Links in the Supply Chain

None of this happens in a vacuum. Today, business computer systems are connected to other business computer systems (a fact that has worried the Pentagon, for one, about the vulnerability of defense contractors to hackers).

Many of San Diego's small businesses are part of much larger supply chains, Easterly observed. The businesses are "part of these key sectors like life sciences, tourism and defense." She then asked Miguel Sampo about supply chain risk, and how the business community might create greater resiliency.

"I work for MasterCard and we see all sorts of stuff," Sampo said.

San Diego has a diverse economy, he said. "We've got the military here, defense, we've got financial institutions, manufacturing, we're a border town right next to Mexico, we've got retail, huge tourism and hospitality [businesses]. … Attackers aren't necessarily just picking one or the other," he said. "If you've got information, it's going to make [you] a target."

When hackers choose a target, they are asking themselves, "Which is the weak actor? Which is the one that's not protecting themselves?"

Sampo's business — RiskRecon, a MasterCard Company — uses its technology to go out and understand which is the weak link in the chain.

"The days of just having great antivirus and a great firewall? Those days are long gone," he said. "That's a product of the '90s. You not only have to worry about protecting your castle, but you have to also worry about protecting yourself [and] who you're doing business with.

"Who are these supply chains? Who are these vendors and what do they look like?" Sampo asked. "Because if an attack was to come through one of those vendors and make their way into me, how do I protect myself from that? How do I make sure that my vendor is doing all the right things to keep me protected as well?"

He introduced the term TPRM — Third Party Risk Management.

"I'm seeing contracts being written that when Company A is going to do business with Company B, there's language that's going in now that says, 'If you're going to do business with me, we use a vendor risk management tool, … a TPRM tool that we use regularly. And we run scans and assessments. If you want to continue to do business with [us], we're going to ask that you maintain a certain grade, a certain level of hygiene.'

"So when you ask me about the resiliency, it's about collaboration," Sampo said. "It's about holding your vendors accountable, understanding how [they are] securing their infrastructure, their assets."

Action Items

Easterly thanked the panel members who participate in regional resiliency programs, such as those that CCOE has undertaken with the cities of Carlsbad and Vista.

She then asked panelists about steps every business can take to help mitigate the risks they have discussed.

"Every business must recognize that they really are a digital business," said Sai Huda. "Who doesn't have a website these days? Who doesn't use email? Who doesn't have a provider that stores data for them on the cloud or on their network?"

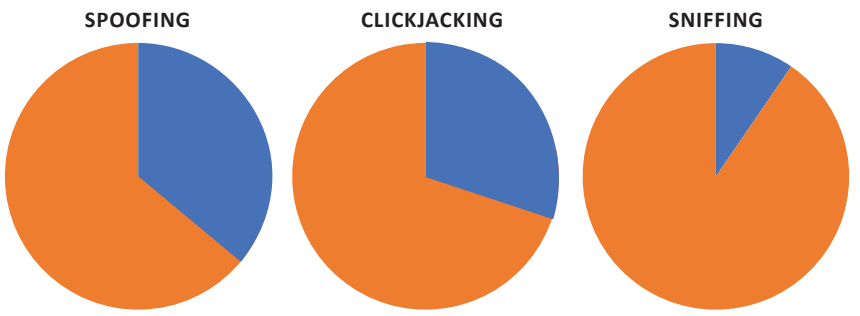
As digital business, he said, they have cyber risk, which is the risk that an attacker will break in. "They'll break in either through an employee by fooling them with a phishing email or having them download malware, allowing the access, or they will break in from outside."

They are either trying to steal data, or infect a system with ransomware so they can demand a payment.

Huda delved into the topic while researching his book, "Next Level Cybersecurity."

Business Vulnerabilities

20,000 SMBs spread across 10 SMB segments in the United States were randomly sampled, and following rates of Vulnerabilities were detected:



SPOOFING	CLICKJACKING	SNIFFING
32.77%	**27.94%**	**10.57%**
6,553 OUT OF 20,000 SAMPLED	5,558 OUT OF 20,000 SAMPLED	2,114 OUT OF 20,000 SAMPLED

Source: SMBVR (Small and Medium Sized Business Vulnerabilities Report, CyberCatch, Q4 2021

Five Steps

While tracing hundreds of hacks for "Next Level Cybersecurity," Huda saw a pattern. "What I discovered is that there are going to be signals" — signals that business people can pick up on, telling them there is trouble ahead.

He lays out 15 signals in the book. Some are very technical.

There are also five steps that every attacker goes through.

"It's just the way the process is."

The first step is reconnaissance. "The attackers will examine you from the outside and your suppliers. Then once they figure out how to break in, they'll break in. That's the intrusion step, the second step. The third step is then lateral movement. Once they're inside your local area network or your cloud, they're going to move on. They have got to find out: Where is the data? Where are the crown jewels?"

Step four is command and control, "which is where they want to figure out a way to either inject the ransomware or extract the data. So they're going to try to connect up with one of their servers outside, undiscovered. And then, finally, the bad deed, which is either exfiltration or ransomware infection."

The Crown Jewels in the Tower

Knowing this, an executive who has not yet updated a company cybersecurity plan has a good set of questions to begin with:

Where are my crown jewels? What are my crown jewels? And what controls do I have in place to prevent, detect and respond to an event?

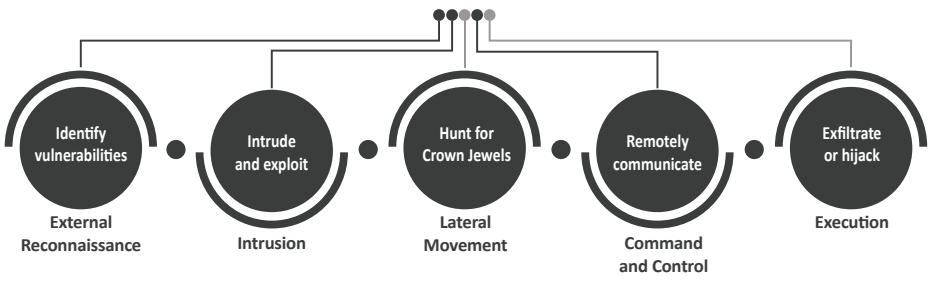
What is our current posture? What are the gaps? What are the blind spots? And how do I mitigate all that?

The point is to get to a stronger cyber risk posture, Huda said. That, however, is not the end of the exercise. "Then you've got to continually test those controls to make sure nothing is broken, or is ineffective, or is missing. And then if you find that [something] is missing or broken or ineffective, then fix them. That's what we do at CyberCatch. We help businesses implement their necessary controls and then continuously test them with our platform. We find the holes so attackers cannot find them and exploit them,"

Huda also recommends companies do a tabletop exercise and run through a scenario like ransomware — again, to find gaps and blind spots, and to mitigate them. "So when the real nasty thing happens, you're not going to be suffering a big damage and be able to quickly recover. [So you are] able to find things like, 'Oh, guess what? I have some backup files that are labeled dot-BAC. So the ransomware can easily scan and find them and encrypt them.'

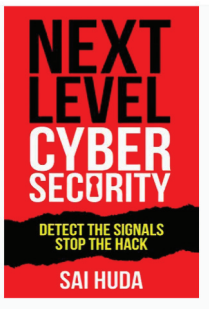
If backup files are offline and off-site, how easy is it to put them back up? If

CYBER ATTACK CHAIN



In his book ***Next Level Cybersecurity,*** Sai Huda, explains the cyber attack chain comprised of five common steps in a hack and reveals 15 signals of attackers if detected early in the cyber attack chain can stop a hack. Here are 5 of the 15 signals:

- ❖ Remote Desktop Protocol (RDP) anomalies
- ❖ Abnormal logons
- ❖ Server Message Block (SMB) anomalies
- ❖ Deletion of backup files
- ❖ Unusual logs behavior

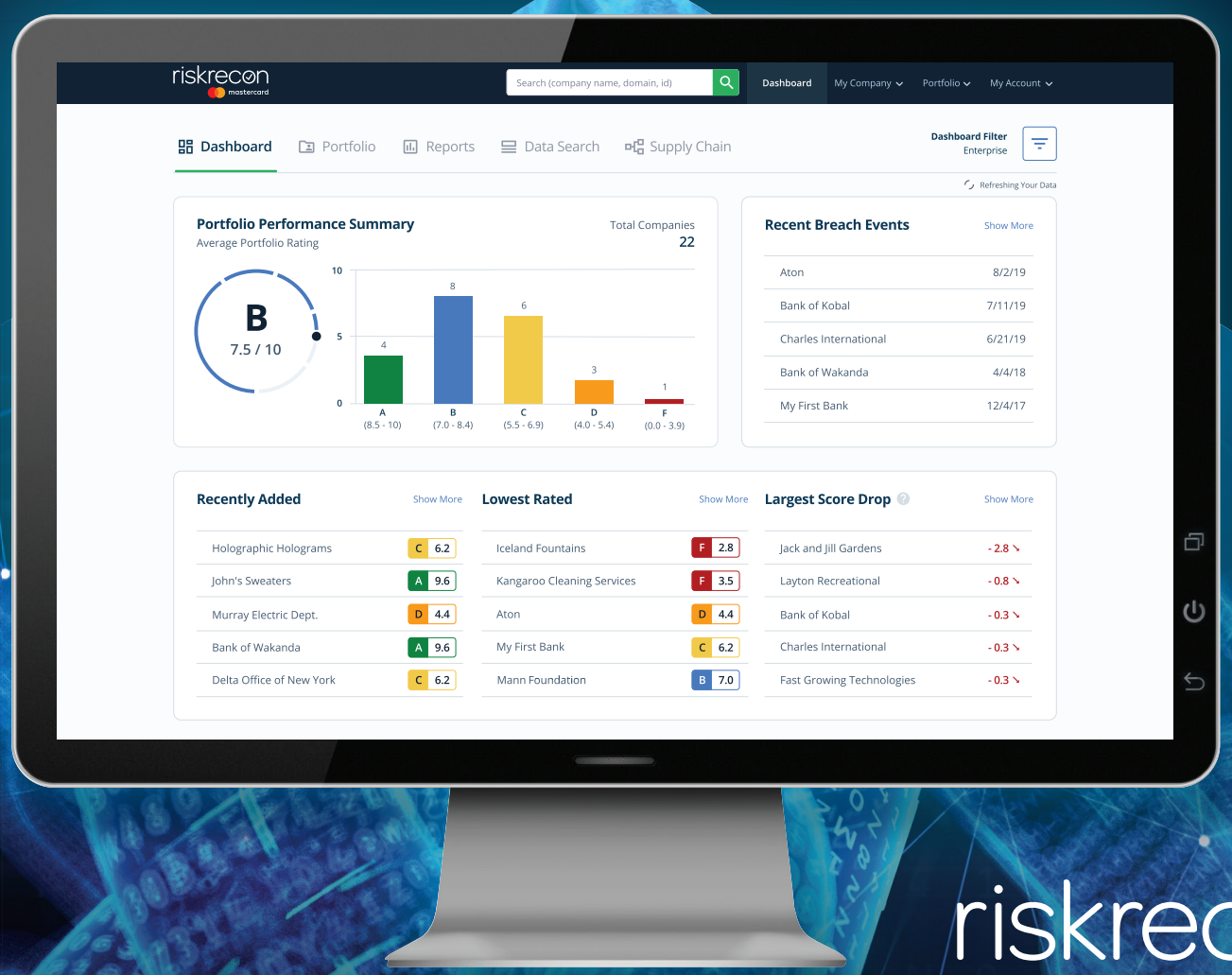


Secure Your Digital Supply Chain

As a cybersecurity professional, making agile decisions with limited information is no easy task. Fortunately, RiskRecon lets you analyze the security performance of your digital supply chain.

During our 30-day free trial, you can get a detailed view of the risks of up to 50 companies in your provider ecosystem, allowing you to make more informed decisions based on risk data.

Start your free trial at www.riskrecon.com/know-your-portfolio



riskrecon
mastercard

it's not easy, a business has a problem.

"So all those little chinks in the armor you can find in a tabletop exercise, and then you're better prepared. So that's a really good MIS risk mitigation tool that I would recommend to every single organization."

Adding AI to the Mix

"You don't want to be having this conversation in the middle of the attack," Easterly said.

Yet she noted that many companies "don't even know where to start" their cybersecurity journey. She then asked Miguel Sampo to discuss how technology might help IT professionals, given the global shortage of cybersecurity professionals.

"I'm a big believer in this thing called AI — artificial intelligence," Sampo said. "How do we do more with less in a world where manpower is becoming very expensive? There's a shortage of cybersecurity professionals. The way to do this is leverage technology."

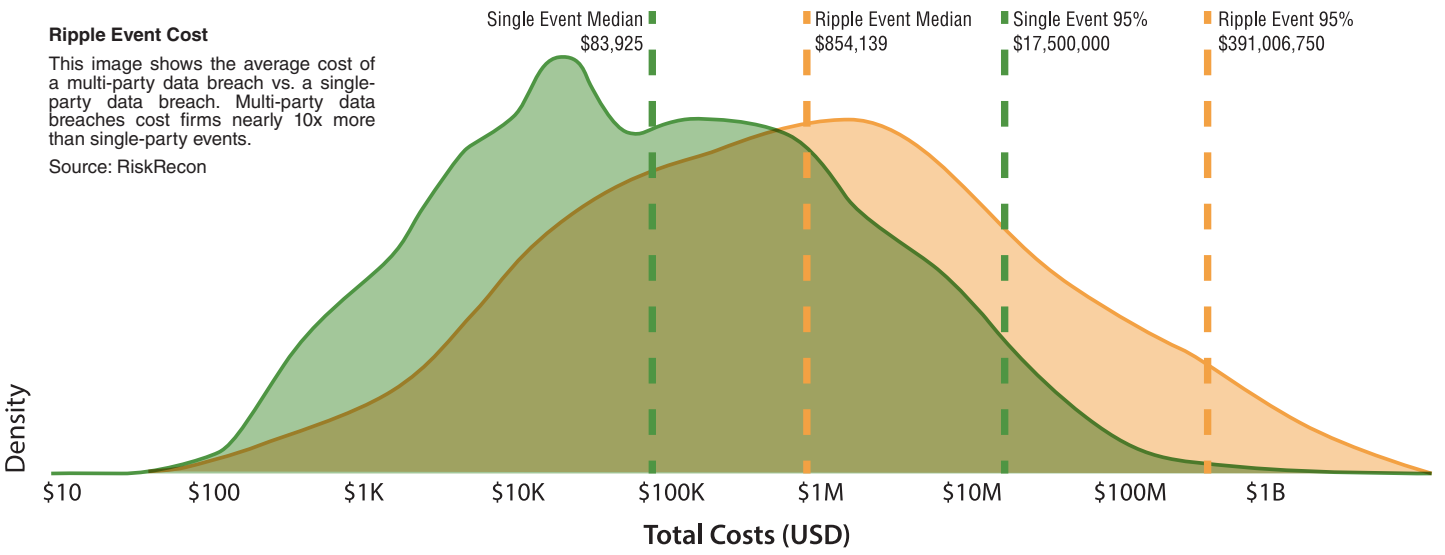
An example of such technology is the RiskRecon platform.

"For example, you don't need to add more heads," Sampo said. "This is not a scenario where you need 15 people running a team, eyes on glass, 24 by seven. You can leverage technology. Like in our case, it would be RiskRecon, a platform that will go out and scan the internet, just like the bad guys do. We scan the internet for these publicly facing machines and servers, understand where are there machines that are vulnerable machines that haven't been patched, where somebody hasn't done due diligence, and making sure that the machines are taken care of.

"I believe [that] leveraging AI is a great return for organizations. You can now take heads that you may have allocated towards this project, use the technology and reallocate those heads to other pertinent pieces of your IT, or other parts of your business to give you a significant return."

Such technology can alert a company representative when there is anomalous behavior or a suspicious change, he said. "For example, with RiskRecon, you have scoring. If you are monitoring a set of vendors and you want them all to maintain a certain level of grade, and you see that grade fall, you get an alert. Now you can go look at it and say, 'Oh, what's happened here? Maybe I've got to keep my eyes on this guy or guys or gals and see what's going on.

"I'm a big believer and I love the whole AI piece," he continued. "I think more and more, we're going to see more AI technology-driven platforms becoming mainstream."



The Human Element of AI

Easterly noted that CCOE recently conducted a study with the **San Diego Regional Economic Development Corporation**, and found that San Diego's cyber industry is employing AI at three times the rate of any other industry.

"And the good news is this is not eating jobs," she said. "We're actually seeing considerable growth within the industry from a jobs perspective. What it's actually doing is providing opportunities for expansion and growth. And that's at that mid-level, allowing us to evolve some of these IT roles and cyber roles, while then still being able to open those positions to this pipeline [of talented people] coming in.

"So, AI is a great opportunity for growth within this industry."

She then turned to SearchBug's Andre Polakoff, and asked how a small tech company might deal with cyber threats.

Getting Help From Big Tech

"My first advice would be minimize exposure," Polakoff said. "So just look at data that you have that is sensitive or could be a target, and encrypt it — at least. Back it up and encrypt it: passwords, credit cards, any other sensitive information. So that's the primary areas of concern.

"There are even better options for passwords and credit cards. Don't store them on your servers. There are ways to do that. Like we added log in with **Google**, log in with **Facebook**, log in with **LinkedIn**. So this way we authenticate a user at Google or LinkedIn. ... And we trust LinkedIn that this is that business account. They don't need to provide a password on SearchBug, and their passwords will not be stored." Companies such as Google or Facebook are protecting your company, he said: "They're not sharing any information except that you are [you]; they authenticated you.

For payment processing, he recommended solutions from companies such as **Stripe** or **Braintree**. "They provide you with easy code you put on your website and this small window is connected directly to the credit card provider — so the credit card number never touches your servers" and there are no worries about credit card theft.

Polakoff also recommended analyzing logs to see if a hacker is snooping. "They may not know what technology a website is, what kind of databases you use. So they will try to use different commands that go with the different operating systems and whatever — to see if a website responds."

Watch out if you see someone trying to access pages that don't exist on your website, or are related to a completely different technology.

"Know those footprints," he said.

He turned again to what he called his favorite topic: SQL injections.

"We got hit really hard many years ago. Nothing was stolen, but we saw all the effort that was put in. So what did I do? I went on the internet and found SQL injection tutorials."

Using that, the entrepreneur built a library of keywords that attackers use to probe and attack a site. Now, if an outsider tries to use a certain keyword, Polakoff knows to block the IP address.

He also noted that SearchBug can give the business community a sense of whether the people they do business with are legitimate. SearchBug can verify whether certain names go with certain phone numbers or addresses; whether emails are fake; or whether phone numbers are active.

"My main point is just, you have to stay vigilant and stay proactive," Polakoff said. "Like if something happens, don't let it go by. See why it happens. It could have been an attempt to penetrate your website. Pay attention to details and thoroughly analyze what happens, because you may find something that you can fix."

Closing the Loop

Asked for final thoughts on the risk landscape and possible solutions, panelists had this to say:

Sampo said the risk landscape is changing. Adversaries are becoming more sophisticated, and changing all the time.

"Is it going to be possible to stay in front of the bad guys? Probably not," he said. "The bad guys are always going to have a leg up, but understanding and protecting yourself and invoking mechanisms — Andre laid out multifactor authentication — and using things like AI, using new technologies to stay out in front as much as we can, is going to be critical."

"I can't tell you how many times I have conversations where a small company says, 'We're not that big. We don't need that. We don't have to worry about that.' And then six months later they're calling because they have a problem."

Companies might be forced to beef up their security because they can't get insurance otherwise, he added.

Huda said cyber vulnerability is becoming an "existential threat." He recounted the story of a small medical practice that fell prey to ransomware. A doctor tried to tell the hackers the business was saving lives. "The attackers laughed and said, so what, you got to pay," Huda said. "The doctor said, no, we're not going to pay you." In the end, the practice shut down.

The threat is real, Polakoff said.

"If it didn't happen to you, it will happen to you."

Some intruders prefer to break in and leave the door open so they can strike later, he noted.

Business owners need to talk to their IT staff and ask questions about potential vulnerabilities, he said. If nothing else, it lets the IT staff know the top people at the organization feel strongly about the topic.

There is outside help available, he also said.

A good resource is the Cyber Center of Excellence, Easterly said. "We have a tremendous plethora of resources on our website, SDCCOE.org, that are all free. And we can provide connectivity into this tremendous ecosystem" of San Diego companies, she added.

That ecosystem includes companies such as CyberCatch, RiskRecon and SearchBug.

More cyber panels are scheduled for later in the year. ■

Table: Change in Cybersecurity Conditions in Internet-facing Systems At Time of Ransomware Detonation Compared with One Year Later

	Day of Ransomware Event		One Year Later	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of Medium or higher (7.0 - 10)	percent with critical issues	56%	49%	12% better
	average issue count	13	11	15% better
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	percent with critical issues	32%	48%	50% worse
	average issue count	4	6	50% worse
Application Security Issues Missing common security practices in applications that collect sensitive data	percent with critical issues	53%	55%	4% worse
	average issue count	8	12	50% worse
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	percent with critical issues	72%	70%	3% better
	average issue count	45	46	2% worse
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	percent with critical issues	67%	58%	13% better
	average issue count	11	9	18% better

This graphic shows the areas in which organizations that have been hit by a ransomware attack actually got worse since their event.

Source: RiskRecon

HELP SAN DIEGO LEAD THE CYBER CHARGE

The Cyber Center of Excellence (CCOE) is a nonprofit that supports the growth of the cyber industry, promotes cybersecurity in San Diego and provides a template to mobilize other regions.

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 CCOE of Excellence