Understanding the Post-Pandemic Cyber Threat Landscape

CYBERSECURITY: A Recap of the San Diego Business Journal's Panel Discussion

■ BY BRAD GRAVES

In an effort to inform and help the wider business community understand the complexities of cybersecurity, the **San Diego Business Journal**, in cooperation with the **Cyber Center of Excellence** (CCOE), held a special cyber panel discussion earlier this month. **Lisa Easterly**, president and CEO of CCOE, moderated the 40-minute talk with four distinguished cybersecurity experts.

MODERATOR

LISA EASTERLY

Lisa Easterly became president and CEO of the San Diego Cyber Center of Excellence this spring 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.

Panelists were **Eric Basu, founder and CEO of Sentek Global, founder and CEO of the Haiku Cyber Range and founding board member of CCOE; Miguel Sampo, senior director of global sales with RiskRecon, a Mastercard Company; Chris Simpson, director of the National University Center for Cybersecurity, a NSA and Department of Homeland Security Center of Academic Excellence in Cyber Defense Education; and Jim Skeen Jr., founding president and CEO and current partner with the Lockton San Diego office, founding board member of CCOE, and private sector engagement partner to the FBI, responsible for delivering the ongoing Executive Briefing series.**

A video of the event will be posted July 28 on the San Diego Business Journal website, at www.sdbj.com.

Lisa Easterly kicked off the conversation with a paradox. As the pandemic generates daily headlines of economic strife and workforce reductions, the cybersecurity industry is growing.

"It just continues to grow by leaps and bounds, protecting our data, our critical infrastructure technology and national security," she said. San Diego leads the charge with 874 cyber firms and **NAVWAR**, the **U.S. Navy**'s Naval Information Warfare Systems Command, whose presence in the region not only drives talent attraction, but spurs new company creation and R&D by spending billions annually on developing and securing critical Navy systems.

Readers can take a much deeper dive into San Diego's cybersecurity scene, thanks to a new report from the **Cyber Center of Excellence** and the **San Diego Regional Economic Development Corporation**. The report also covers the growth of artificial intelligence and machine learning. Titled "Securing the Future: AI and San Diego's Cyber Cluster," the report is available on the websites of both organizations at sdccoe.org and sandiegobusiness.org.

The numbers in the report are impressive. Easterly noted that the cybersecurity cluster accounts for more than 24,000 jobs, 12,400 cyber-specific roles and has an economic impact of $3.5 billion annually. "Put simply, the impact of the cyber industry on the region here is equal to hosting nine Super Bowls or 23 Comic-Cons," Easterly said. "As a Marvel fan, that makes me smile."

She noted that the secret to San Diego's success is the collaboration between industry, academia and government. That seeds a talent pipeline for high-paying jobs to the tune of about 22,000 cyber related degrees conferred each year. Out of this fertile environment come new technologies and solutions to combat the cyber threat, which continues to evolve.

Easterly noted that since the pandemic began, the **FBI** reported a 300% increase in cyber crimes with **IBM** estimating the average cost of a breach climbing over $3.8 million. With that, she asked panelists about the biggest cyber threats facing the industry today.

Jim Skeen Jr. is fond of using visuals when discussing cybersecurity. "Think about your business for a minute," he said. "Let me ask you to visualize the Olympic rings, that logo stenciled on a white tablecloth, each ring representing a key function in your business: IP, finance, IT, legal and operations.

"Now pretend that you just spilled a big pitcher of red wine on that nice tablecloth, and that represents a breach. It could be internal, it could be external, but it's permeating each of those functions at the same time. And the question really becomes, do you and your business have a plan, a plan for each function, and then is that plan rolled up and interoperable for an incident response? In other words, are you ready?

"Some of the biggest threats that come to mind for me right now would be obviously the stuff about extortion and ransomware. It's rampant. It's creating a tsunami-like effect on law enforcement, trying to keep up with it. Of course, there's business email compromise, theft of your IP, all the issues related to social engineering fraud. And don't leave out, of course, the regulatory landscape and political risks. There's an awful lot going on that the cyber industry is trying to contend with at the same time. Much of it is quite unprecedented."

Eric Basu turned the conversation back to the first threats that Skeen mentioned. "What are the big dollar losses that businesses are facing today? It's ransomware," Basu said. "I think the **Colonial Pipeline** [incident] is something we're all aware of. That was a relatively big payment. It's wire fraud. That's an old school … it's an oldie, but goodie, if you would. … But a lot of our commercial customers are still running into that."

Intellectual property theft, he continued, could have a longer term effect on the bottom line of a company. It is a loss either of market share or of actual dollars.

➡ *Cybersecurity page 16*

THE PANELISTS

ERIC BASU

Eric Basu is CEO of Sentek Global, a technology services provider for the U.S. government mainly related to IT security program management. He is a former U.S. Navy SEAL commander who holds an MBA from the Anderson Graduate School of Management at UCLA. Basu launched Sentek out of his home in 2001 and the company now employs nearly 200 individuals. He also founded the Haiku Cyber Range, a gamified cybersecurity simulator that teaches real world cybersecurity skills via a game interface.

MIGUEL SAMPO

Miguel Sampo is senior director of global sales with RiskRecon. Sampo has more than 20 years 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.

CHRIS SIMPSON

Chris Simpson is director of the National University Center for Cybersecurity and academic program director for the master of science in cybersecurity program at National University. Simpson has developed innovative curriculum and labs in ethical hacking, penetration testing and incident response. He retired from the U.S. Navy in 2009 after 27 years of service. He holds a bachelor's degree from the University of Maryland and a master's degree in information security and assurance from George Mason University.

JIM SKEEN JR.

Jim Skeen Jr. is founding president and CEO of Lockton San Diego. Skeen has more than 40 years of experience successfully navigating complex risk factor solutions for verticals such as AIML, basic research, communications, construction, cybersecurity, defense, healthcare, hospitality, life sciences, M&A, real estate, retail technology and workforce solutions. He dedicates significant time and expertise to cyber risk awareness and is a founding board member of the Cyber Center of Excellence. He is a private sector engagement partner with the FBI.

HELP SAN DIEGO LEAD THE CYBER CHARGE

The Cyber Center of Excellence (CCOE) is a nonprofit dedicated to growing San Diego’s cybersecurity presence.

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.

Lisa Easterly, CCOE President & CEO

Get involved at **sdccoe.org**.

ACCELERATING THE CYBER INNOVATION ECONOMY

Cyber Center

CCOE

of Excellence

Cybersecurity

➡ from page 14

A related concern is business continuity. Hackers are able to separate businesses from the vital information they have on their computer systems. In many cases that data is not backed up. "The reason people pay," Basu said, "is because they don't have business continuity anymore." Other threats include insider threats, denial of service and hacktivist attacks.

Basu then turned to the topic of risk mitigation, which, unfortunately, is never perfect. "There is no way to completely protect your systems from ever being compromised. It's not going to happen. It's not a realistic solution. And so the ability to mitigate the risk, the ability to try to avoid the risk and then mitigate the risk through a combination of things [is key]. And it's policies and procedures. Also, having the right insurance is key."

Following that, **Lisa Easterly** asked panelists who in San Diego might be a target for hackers. "San Diego is home to a vibrant innovation economy, tourism industry and a very large concentration of military assets — actually one of the largest in the nation — which creates a bullseye for bad actors."

"Unfortunately, I think every industry is actually a target," said **Chris Simpson**, "because in many cases, the attackers are looking for easy targets to get in and steal information or steal financial data, credit card data and things like that." He mentioned the tourism industry, which handles a lot of payment information on its servers. San Diego's status as a port city and a Navy town also makes it a target for hackers with specific agendas, including those sponsored by nation states. One **U.S. Navy** command based in San Diego, **NAVWAR**, specializes in information technology and cybersecurity.

Simpson turned to one common hacker trick: targeting a small institution to get to a bigger one. It is possible because so many businesses and institutions are interconnected. The **Department of Defense,** he noted, is supported by a lot of small contractors. "So in many cases, the attackers try to go after the small organizations to gain a foothold, to get into the bigger contractors. So that that's definitely a consideration for the small organizations, and that's not just DoD, a lot of small companies support bigger companies."

Bad actors, **Miguel Sampo** said, are not playing favorites. "They're looking at *everybody*. So when I think about what industries are vulnerable, *everybody's* vulnerable right now." The healthcare industry is particularly vulnerable, he said, alluding to a high-profile breach in San Diego, but noting that hackers are targeting healthcare organizations worldwide.

Another target, he said, is the finance industry. Then he turned to what he sees as a change in attitude among hackers: "These bad actors aren't motivated anymore, as they were back when I started 23 years ago, just for notoriety or fame. They're doing it for money. There's big money behind this." Hence, the interest in finance targets.

"Miguel, you said something really interesting," **Eric Basu** said. "We're seeing a change from what it used to be. You used to have people who were going out for just trophies and you have the hacktivists who really were interested in a mission. And then you had the state actors who, almost with a 'holier than thou' attitude, [said] 'We're only after infrastructure. We're not going after money because we're not criminals.' That's all blurred now. [Consider] the Colonial Pipeline. Russia, of course, says it was not a state-sponsored group that did that, but there is no Russian criminal organization that survives in that country without the implicit permission of the government. It's a relatively totalitarian country. They just don't exist. Same thing in China. You don't have criminal groups that exist in China without the government at the very minimum looking the other way.

"And so we now have criminal organizations that are actually doing infrastructure attacks, and they're trying to get money out of it. We have government organizations that are looking at it going, 'as long as we're attacking it anyway, why don't we make money out of it?'"

Bottom line, it comes down to money.

"Eric makes some great points about organized crime and some of the blurring of organized crime with state sponsorship," said **Chris Simpson**. "So there's a great report that **Verizon** does every year. It's called the Data Breach Investigations Report. And it's not really technical, so if you're just a small business leader, it's actually a pretty interesting read. But they noted in the most recent one, 80% of the attacks are financially motivated by organized crime and they want to go in and they want to steal financial data."

What is interesting is that bad actors are targeting old software with known vulnerabilities. "So they had a neat chart. Most of the vulnerabilities that were targeted for are from 2010. So Eric mentioned risk mitigation a little earlier. If you can remove some of the older vulnerabilities, which is rather easy to do, you can reduce that attack surface."

A second thing hackers are after is credentials: "They like to get passwords because many people typically use a password in more than one place. So if they get your password on Gmail and you use that for your work account, they'll use automated tools to try to get into those systems. It's all efficient. They're actually very automated, very organized. It's really an industry in some ways, that they're going out and they're going to scan everybody out there and try to get into as many systems that they can, and then steal that financial information."

The important conclusion from all this, **Lisa Easterly** said, is that cybersecurity is everyone's business. The question becomes what can companies do to increase their cybersecurity posture and also help mitigate risk?

"Risk is when you make a bet and if you get it wrong, it may hurt," **Miguel Sampo** said. "It may hurt a lot." Those were the sentiments of the French gambler and mathematician Chevalier de Méré during the 1600s. With that, Sampo turned to the topic of cyber hygiene — an issue that his company, **RiskRecon**, deals with extensively.

"It's almost one of those terms that sounds so nebulous nowadays, but what does cyber hygiene mean?" Sampo said. "It means a lot of different things. But more importantly to us, … it's understanding what practices, what tools do you have, what security controls have you put in place to try to mitigate that risk, and not leave a door unlocked, a window open, kind of thinking of like a Neighborhood Watch kind of analogy."

Cyber hygiene should include items like timely software patch management, and understanding what security controls a company has in place. "Are you using web encryption? Are the servers that you have that are publicly facing and exposed potentially to the bad actors, are those protected? Are those locked down? If a machine was to be compromised, do you know the value of that system?" A low-level server, he noted, is much less valuable to a bad guy than, for example, a web mail server or a content server that has personally identifiable information that somebody's logging in.

He mentioned **RiskRecon** is working with the city of Carlsbad and CCOE to help small companies improve their cyber hygiene.

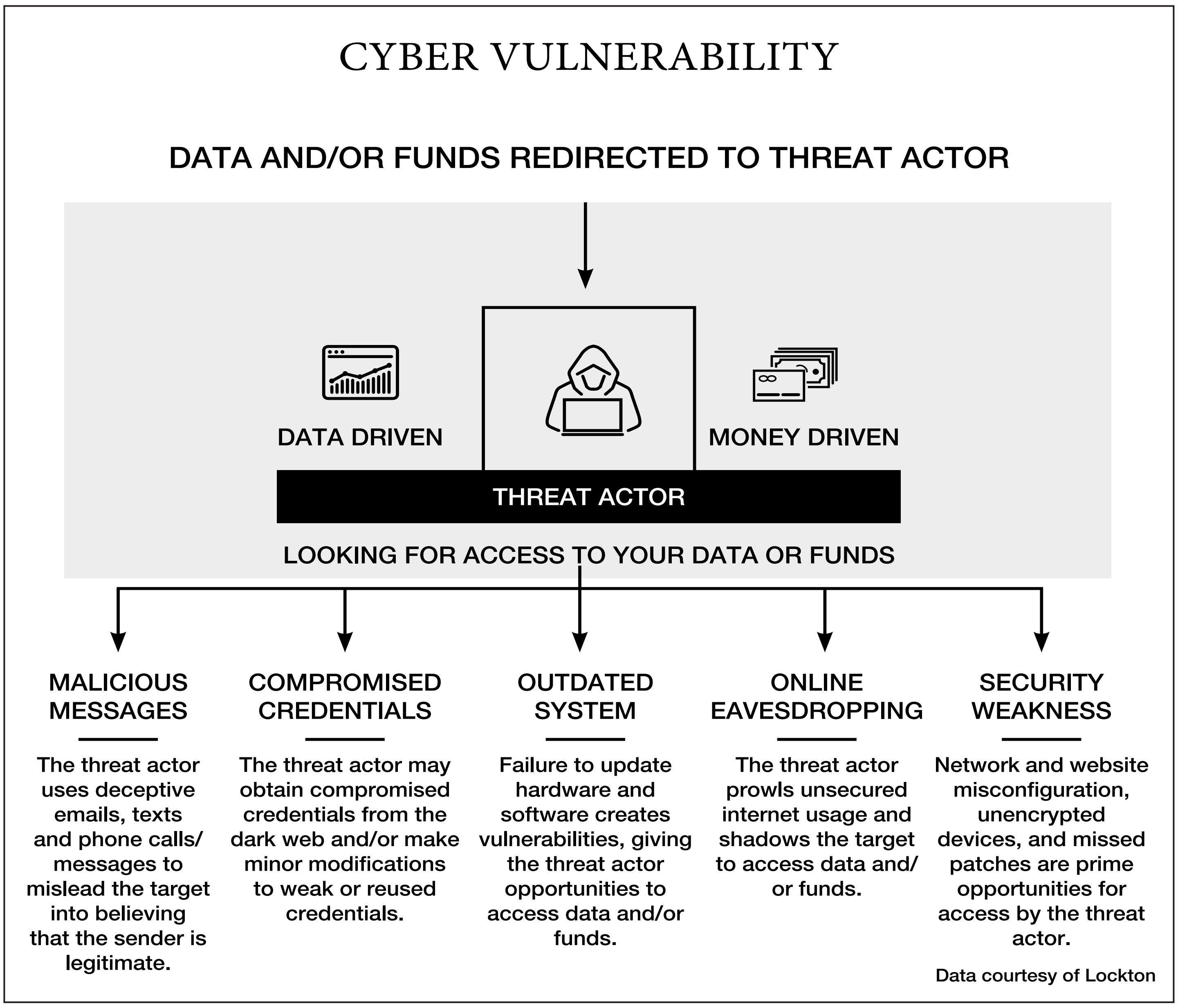
In assessing vulnerabilities, he said, be aware of who you do business with. "We're connected in so many different ways online," Sampo said. "It's no more the soda pop delivery guy dropping off sodas anymore. We're doing everything online. And so when we think about those assessments and the interconnected world that we're in, understanding where there's gaps at every one of those points or vectors is absolutely critical. …"

"Some of these breaches that we've seen recently aren't a result of an organization's antivirus and firewall that failed. It was a lack of visibility into the risk that was introduced by somebody that they never even thought about," he said.

Businesses don't necessarily know what they don't know, said **Lisa Easterly**, and so doing a real assessment of one's business and its risk is valuable.

Jim Skeen Jr. then spoke about the realities and trade-offs that businesses face, and turned to the issue of cyber insurance. "It's such a daunting task for our IT professionals and how they

➡ Cybersecurity page 18



CYBER VULNERABILITY

DATA AND/OR FUNDS REDIRECTED TO THREAT ACTOR

DATA DRIVEN

MONEY DRIVEN

THREAT ACTOR

LOOKING FOR ACCESS TO YOUR DATA OR FUNDS

MALICIOUS MESSAGES

The threat actor uses deceptive emails, texts and phone calls/ messages to mislead the target into believing that the sender is legitimate.

COMPROMISED CREDENTIALS

The threat actor may obtain compromised credentials from the dark web and/or make minor modifications to weak or reused credentials.

OUTDATED SYSTEM

Failure to update hardware and software creates vulnerabilities, giving the threat actor opportunities to access data and/or funds.

ONLINE EAVESDROPPING

The threat actor prowls unsecured internet usage and shadows the target to access data and/ or funds.

SECURITY WEAKNESS

Network and website misconfiguration, unencrypted devices, and missed patches are prime opportunities for access by the threat actor.

Data courtesy of Lockton

Lockton Global Cyber & Technology

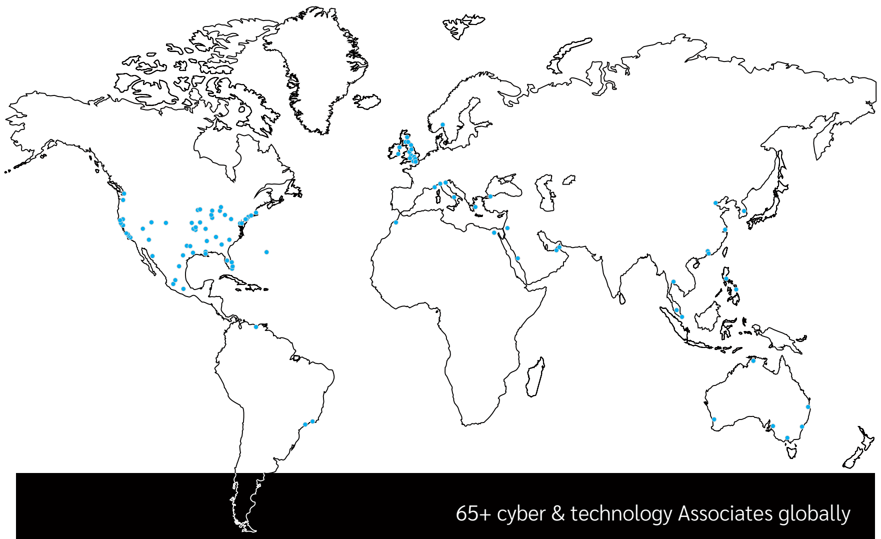
Global Cyber & Technology Team

AS THE WORLD'S LARGEST PRIVATELY OWNED, INDEPENDENT INSURANCE BROKER. LOCKTON'S INDEPENDENCE GIVES US THE FREEDOM TO BE A STRONG, FLEXIBLE ADVOCATE ALWAYS ACTING IN THE BEST INTEREST OF OUR CLIENTS, CREATING AN ENTIRELY DIFFERENT DYNAMIC — ONE THAT'S FOCUSED ON YOUR SUCCESS. Led by a premier team of cyber brokers and advisors, Lockton's Global Cyber & Technology team is dedicated to delivering unparalleled service and innovative programs for your organizational needs.

Supported by cyber claims experts, former security practitioners and legally qualified technicians, our global team offers a wide range of expertise in risk identification, protection and management, as well as proven delivery of results.

Our global reach ensures that our clients have access to the knowledge that comes from experiences across multiple jurisdictions and multiple industries.

UNMATCHED INSURANCE AND RISK TRANSFER PROGRAM ADVISORY AND PLACEMENT SOLUTIONS



65+ cyber & technology Associates globally

More than 300 incident handled each year with a 99% covered claim rate to date

Relationships with more than 175 insurance companies globally

Lockton's three-step approach: Inform, Improve, & Insure

NAVIGATING THE BEST CYBERSECURITY SOLUTION PROVIDERS CAN BE OVERWHELMING. That's why you'll be paired with a trusted advisor, who's equipped to lead you through the process.

Inform

ANALYSIS
- Insurance program benchmarking
- Coverage gap analysis
- Data on thousands of insurance programs

ASSESSMENT
- Cyber risk posture and maturity
- External vulnerability scan

QUANTIFICATION
- Data breach
- Business interruption
- Dynamic Capital Modeling
- Bespoke modeling

Improve

LOSS CONTROL
- Cyber risk reviews
- Incident response exercises

RISK CONSULTING
- Data breach scenarios
- Board/executive education and engagement

PARTNERED SERVICES
- Managed detection and response
- Forensic accounting
- Data landscaping
- And more

Insure

TAILORED INSURANCE SOLUTIONS
- Comprehensive risk protection programs with property, casualty, D&O, crime, and more
- Policies crafted to address each client's unique risks

MARKET COVERAGE
- Global carrier relationships and broader coverage provide clients with more options
- Proprietary forms
- Enhancement endorsements

CLAIMS ADVOCACY
- Experienced and forceful advocacy with insurers
- Use claim experience to constantly improve policy language
- Claims administration and support

Jim Skeen, Jr. | Partner, Lockton Partners, LLC | jskeen@lockton.com | 858.587.3200

LOCKTON®

lockton.com |

Cybersecurity

➡ from page 16

get through the process of weighing out budget constraints and priorities for their business versus all the solutions out there. … What's interesting is that notwithstanding everyone's best efforts, there will be residual risk and it could be severe."

He then asked his audience to think of another visual, a city skyline. "Look through the lens of your contractual relationships with other parties. These are your clients, your suppliers, and your vendors, some bigger and more robust than others. But part of the question to ask yourself is what happens when they are breached? What's the impact on your business? If they're no longer functioning, are you also down? Do you have a contingent exposure based on these other partnerships? The answer is yes, you do. And it's worth exploring.

"Over the years, cyber insurance has become a much more common topic. In the old days, 20 years ago, it was just big retailers, utilities and hospitals thought about it, but now it's every day for all of us. I think it's important that everybody take a step back and ask themselves what is an insurance company? It's a big, slow moving, highly regulated, often publicly traded company. It offers in their mind a contract consisting of terms, conditions, exclusions and pricing. And those things are based on decades upon decades of settled case law and countless paid claims as an industry, to which they then apply actuarial science to help figure out the makeup of what they're offering you in exchange.

"The challenge really is those key factors are not present in cyber. It's all evolving and evolving very quickly. It puts a huge pressure on them to try to figure out what to offer and at what price. So it's really a supply and demand issue at its most basic core. And the underwriters right now — based on this never ending tsunami of business email, ransomware, the list just goes on and on and on — they have significantly and recently raised the bar on what it will take for your business to get adequate insurance. And think in terms of three buckets of rates: favorable, standard and unfavorable. Naturally, you want to do what you can within your own priorities and budget to qualify for favorable pricing and rates. But you need a business plan relative to these questions that they are going to ask you right now."

Specific questions an insurance company may have for its customers are in the story below.

Lisa Easterly noted that the audience for this panel discussion has a tendency to be smaller businesses that don't necessarily have the resources of their larger neighbors. "I think the threat landscape is a bit daunting for companies," she said. She asked the panelists about resources available to local businesses. She also

➡ Cybersecurity page 20

Buying Cyber Insurance Requires Careful Study

CYBERSECURITY: There Is Plenty to Think About; Fortunately, Companies Have Resources

■ By BRAD GRAVES

Coming to a decision regarding a company's cyber insurance is no quick exercise. It's not like buying a commodity like toothpaste, said **Jim Skeen Jr.**

Skeen knows a thing or two about insurance — and cybersecurity. He is the founding president and CEO of **Lockton San Diego**, an independent insurance broker in the University Towne Center neighborhood and the eighth largest insurance brokerage in the world. In addition, Skeen is a founding board member of the **Cyber Center of Excellence**, a San Diego nonprofit working to accelerate the region's cyber economy.

With so much cyber-crime in the headlines, leaders of companies reach the decision to buy cyber insurance. The first thing they need, Skeen said, is time to think about options. A company planning to buy its next 12 months of cyber coverage will ideally start the process 100 days in advance, to give themselves the option to make informed decisions well in advance of binding coverage.

The 100-day evaluation process will have to involve a company's legal and information technology teams. Companies will have to mull what risks they can retain versus what risks they want to transfer. The process involves hard decisions as well as trade-offs, Skeen said.

Informed buyers will also anticipate subjectivities. "They are anticipating the insurance companies coming back and saying, 'We need these questions answered before we offer you a quote.'" They should expect a lot of questions about their IT architecture and controls.

In addition, informed customers will expect tradeoffs. They will have to make decisions about the breadth and depth of the coverage, including the limits they would like to purchase, as well as retentions (which are very similar to deductibles). And, of course, rates.

A Seller's Market

As for rates, insurance is a seller's market, Skeen said. "I want to emphasize it's not a seller's market based on greed. It's a seller's market based on uncertainty."

To set their rates, insurance companies pore over decade upon decade of settled case law as well as, in the aggregate, hundreds of thousands of paid claims, to which they apply actuarial science to price their product. But in many ways, cybersecurity is a new frontier: the issues that companies expect to face are just beginning to present themselves. There is no historical record to base rates on.

"The challenge is that we really don't have those things as present relative to cyber insurance," Skeen said. "We don't have decade upon decade of settled case law. We don't have millions of paid claims against which they can price their product actuarially.

"What we have is a real and growing threat that involves not just cybercriminals but also organized crime and nation states, sometimes partnering with one another."

Business people have two more concerns. "In addition to just trying to protect your business, you also have to navigate the regulatory and political risk component of this," Skeen said. California law as well as federal law affects the issue. The **U.S. Treasury** maintains a list of bad actors in the world. "You could be in violation of the law if you paid ransom to one of those bad actors on the U.S. Treasury list," Skeen said. "It's important that each business rely upon the resources provided by the insurance company and its legal team to make sure they stay in compliance with evolving guidance from the U.S. government."

Knowledge Is Power

Let's close with a message that's at once pragmatic and hopeful. Skeen noted that since 90% of the problems we read about are self-inflicted, "that means there's a lot that we can do to better protect our communities, businesses, families and selves in this area. So it's really about division of labor. The more we can take on ourselves as private citizens, the more we free up the limited resources of our professionals in law enforcement — and our IT departments."

There is also help out there, including help from the FBI, which offers briefings about cybersecurity threats. Skeen helps coordinate those briefings as private sector engagement partner to the FBI, delivering awareness, education and actionable steps through the Executive Briefing Series. More details on the series are available through the Cyber Center of Excellence website.

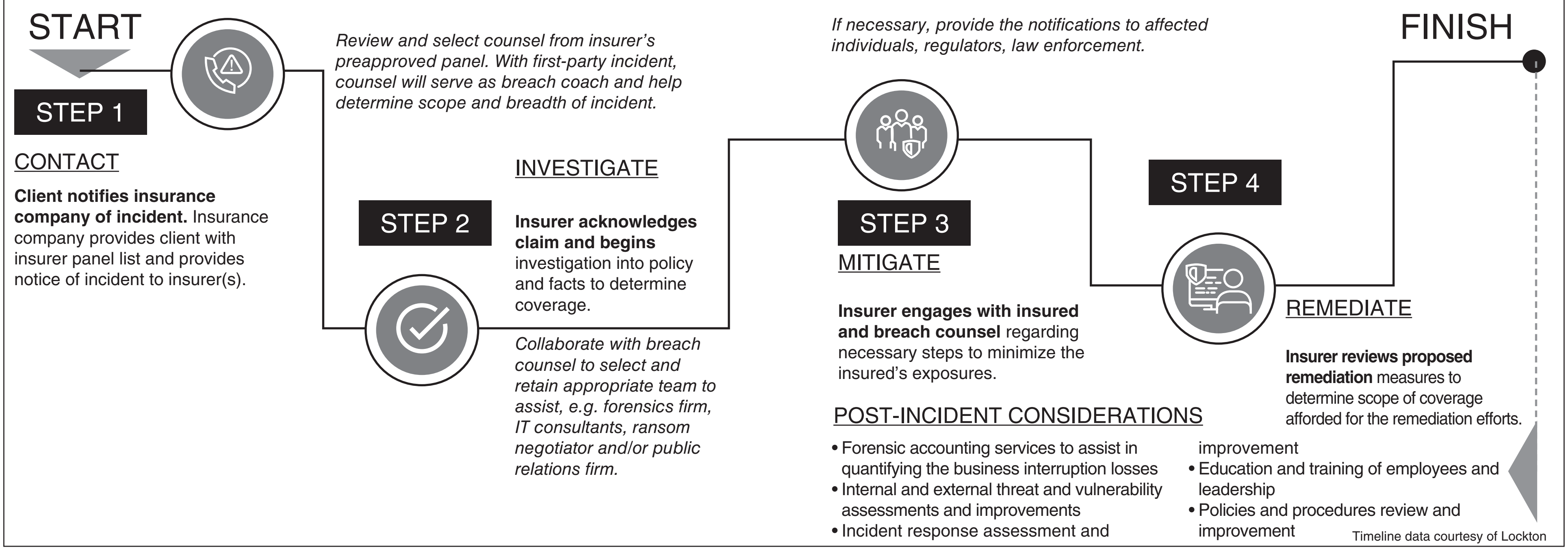
Questions to Expect From Your Insurance Company

In the market for cyber insurance? Lockton's Jim Skeen Jr. advises companies to be ready for questions such as these:

- Is there multifactor authentication for all remote users, access to the cloud and vendors?
- Are users restricted from administrator rights?
- Do you have a robust continuity plan?
- Do you have backup systems that are air gapped and/or encrypted?
- Do you have remote desktop controls?
- Do you offer regular and relevant employee training?
- Do you have a plan in place for patch management, especially "critical" patches, within 24-72 hours?
- Do you have a plan in place for end of life or end of support software, and its segmentation?

What Happens When There Is an Incident?

Process begins upon receipt of a regulatory inquiry, written demand, arbitration demand, and/or complaint OR notice of breach, suspected breach, suspicious activity on the network, security incident and/or ransomware attack.



START

STEP 1

CONTACT

Client notifies insurance company of incident. Insurance company provides client with insurer panel list and provides notice of incident to insurer(s).

Review and select counsel from insurer's preapproved panel. With first-party incident, counsel will serve as breach coach and help determine scope and breadth of incident.

STEP 2

INVESTIGATE

Insurer acknowledges claim and begins investigation into policy and facts to determine coverage.

Collaborate with breach counsel to select and retain appropriate team to assist, e.g. forensics firm, IT consultants, ransom negotiator and/or public relations firm.

If necessary, provide the notifications to affected individuals, regulators, law enforcement.

STEP 3

MITIGATE

Insurer engages with insured and breach counsel regarding necessary steps to minimize the insured's exposures.

STEP 4

REMEDIATE

Insurer reviews proposed remediation measures to determine scope of coverage afforded for the remediation efforts.

FINISH

POST-INCIDENT CONSIDERATIONS

- Forensic accounting services to assist in quantifying the business interruption losses
- Internal and external threat and vulnerability assessments and improvements
- Incident response assessment and improvement
- Education and training of employees and leadership
- Policies and procedures review and improvement

Timeline data courtesy of Lockton

EDUCATION BENEFITS FOR YOUR CYBERSECURITY WORKFORCE

Balkis N., Class of 2019

SCHOLARSHIPS AVAILABLE FOR WORKFORCE PARTNERS

National University is proud to offer no-cost education benefits to workforce partners looking to upskill or reskill their workforce. With tuition reduction scholarships and a unique four-week class model created for adult learners, workforce partners can help their employees expand on the knowledge and skills needed in cybersecurity and a variety of other in demand fields all designed around work-life balance and advancement in their careers.

Targeted Education Solutions to Meet your Needs

- Tuition Reduction Scholarships
- Customized Cohorts
- Targeted Upskilling and Reskilling
- Customized Education

National University Cybersecurity Programs

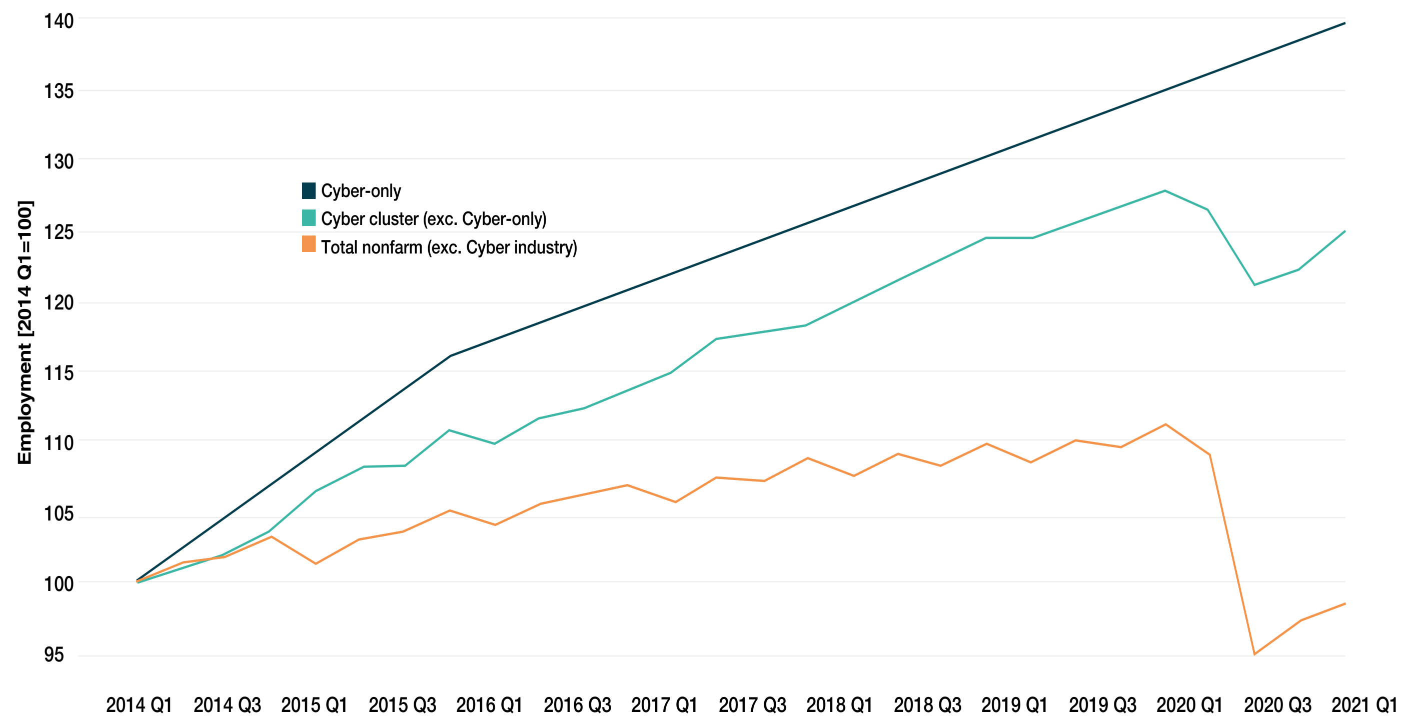
- Bachelor of Science in Cybersecurity
- Master of Science in Cybersecurity (NSA/DHS National Centers of Academic Excellence Designation)
- Workforce Training and Development Cybersecurity Certificates

50 NATIONAL UNIVERSITY est. 1971
NATIONAL
UNIVERSITY
Veteran-Founded Nonprofit for 50 Years

LEARN MORE
WESCorp@nu.edu
(619) 648-0207

JOIN US AS A WORKFORCE PARTNER

Cyber-specific employment growth has outpaced that in other San Diego industries



Sources: BW Research Partnership, U.S. Bureau of Labor Statistics, U.S. Navy Naval Information Warfare Systems Command (NAVWAR), San Diego Regional EDC

Cybersecurity

➡ *from page 18*

asked **Jim Skeen Jr.** to discuss his role as private sector engagement partner for the **FBI**. The agency can be a resource for business.

Skeen said the **FBI** has a 500-person office here led by Special Agent in Charge **Suzanne Turner**. It has the **San Diego Cyber Task Force**, which is led locally and works very closely with the CCOE.

The best way to report an incident to the FBI, he said, is the incident response center at www.ic3.gov. Certain incidents may be investigated by the **Secret Service** which focuses on financial crimes. Both agencies are able to give direction on whether a matter is best taken up by the FBI or Secret Service.

Also of interest is the San Diego **InfraGard** program, sponsored by the FBI. There are 70 chapters in the United States. Membership is free; prospective members are subject to a quick background check. Once enrolled, members get access to "some very valuable information, continuous information and training and networking, on infrastructure issues primarily," Skeen said. "We really encourage someone in your organization to become a member of InfraGard."

Asked about resources for business, **Eric Basu** said the **Cyber Center of Excellence** is an excellent resource and a superb source for referrals. "Whenever I get a question from anybody that says, 'Hey, who do I talk to about this? I've been breached, who do I talk to in law enforcement?' The first thing I do is I go back to the Cyber Center of Excellence."

He recalled that the center was originally founded to be "a one-stop shop where everybody could go to learn about cybersecurity." He added that the tabletop exercises that the CCOE has done — bringing together government, military, business, law enforcement and infrastructure specialists — are just one example of the networking available through the organization.

On a second point, Basu said, "it's more than just knowing who to go to after you've had a problem. The question is proactively, how do I train people? Or for a lot of people, how do I get into this industry? How do I train?" Universities affiliated with CCOE have great programs, he said. " **National University** has one of the most recognized nationwide cybersecurity programs as partners with the **NSA**. And their flexible schedule allows people who say, 'I can't take four years off to get a degree,' it allows them to get a degree while they're working on other projects.

He then brought up his own business project, the **Haiku Cyber Range**. "The idea there was that I would interview people all the time and they would have a certification and have a degree, but they really didn't have any hands-on skills. They didn't know how to get in there and actually, you know, run Metasploit …. So we said, 'there's got to be a way to address this.' So we came up with the idea that maybe there's an opportunity in cybersecurity for an apprenticeship and a journeyman type of set of skills where we're learning like a plumber. I'm learning on the job, I'm looking at how things are done. I'm actually getting the muscle memory and the mental memory of how to do this, and we're putting this together. And so we developed Haiku with that idea and we decided to democratize it and make it available at $14.99 a month so that people can go out there and actually get hands-on skills while playing a game and having fun, so that they can get an entry into this into business, which hopefully leads to high paying jobs, advanced degrees. Hopefully they're our future CISOs 10 years from now."

"And I will say the cyberpunk environment [in the Haiku Cyber Range] is quite fun," said **Lisa Easterly.** "Even as a non-cyber expert by trade, I had a great time playing on the resource."

Chris Simpson continued the conversation by turning to San Diego's academic community. "Our students at National University, they do a three-month capstone project. And one of the things that we offer is they'll go out and they'll help a company improve their cybersecurity. They'll do assessments, they'll do pen tests [penetration tests], they'll write policy. And the great thing is it doesn't cost anything. So it's free work and it's a nice way for a university to get up to kind of a baseline and then maybe find a managed security service provider that they can kind of hand that work off to. And it's not just our university. So **Cal State San Marcos**, they do this, to a **University of San Diego**, **San Diego State**. There's really a robust academic community here. And we also have some great security organizations [including] **ISACA**, which is kind of the auditing security management side.

"I would just like to add about building the workforce … don't forget about high school," Simpson continued. "We help with the SoCal Cyber Cup, a high school, middle school and community college cyber competition. And it's a great way for high school [and] the younger students to learn. They're really impressive. We've used a Haiku Range as part of that competition before. And it was a great training environment for them to really, like Eric said, get their hands on and learn. And it's amazing how well these young students work together as a team. So if you're a parent, I'd encourage you to get your kids involved in some of these different cyber competitions because it's a great career field."

One more resource for businesses to train their workforces, Simpson said, is free training offered by San Diego cybersecurity software provider **ESET**. "You look at a lot of the breaches, it's all social engineering and people just being tricked," he said. With awareness, he said, people will not click on suspect links, or give out passwords to strangers on the phone who claim to be from Microsoft.

Miguel Sampo then spoke about the resources that his company, **RiskRecon**, can offer.

"We provide different types of trials, different types of pilot programs … . That's one of the beauties of having all these tools available online. There are a lot of different ways to arm yourself and prepare yourself. But we absolutely would love to be able to talk to any and all about how do we help them with their program, their cybersecurity program, and integrate something like third-party risk management [also known as TPRM]. It's becoming more and more mainstream and a necessary component, just like an incident response retainer, just like having cybersecurity insurance, just like having a firewall. TPRM is becoming more mainstream."

Sampo also had thoughts about the cybersecurity industry in general: **"**I tell folks that this discipline that we're in, it's a huge industry, but a small community. And at the end of the day, we all want to help each other as much as we can."

"We love partnering with the CCOE," he said. "You guys have a lot of great programs."

"Visit us online and come check us out," Sampo said of **RiskRecon**. "We can also offer a lot of different things. But I would tell people, take a look at what's out there. How do you make your program a little stronger and add some more pertinent pieces to your cybersecurity strategy?"

"I think the key takeaway for our audience is that San Diego has an incredibly robust cyber ecosystem," said **Lisa Easterly**. "We're the biggest small town and are good at operating with all hands on deck. Throughout San Diego's innovative history, we've seen industry, academia, local government, and the military collaborate to not only develop these clusters, but to sustain, grow, and now protect them. Today, we gave our audience a good overview of the post-pandemic threat landscape—including vulnerable industries—ultimately coming to the conclusion that cybersecurity is now everyone's business.

"We've talked about who's after this data, what kind of data they're after, and what it is that you need to be protecting. And then once we scared everybody, we talked about the resources that are available and how folks can start to look at mitigating their own risk.

"Thank you so much to our panel, Eric, Chris, Miguel and Jim. It's been phenomenal as always to speak with you." ■

For More Information …

Executives wanting to learn more about cybersecurity have a wealth of options. The following is a list of resources, including a newly announced initiative from the U.S. Department of Homeland Security. The list was compiled by the Cyber Center of Excellence.

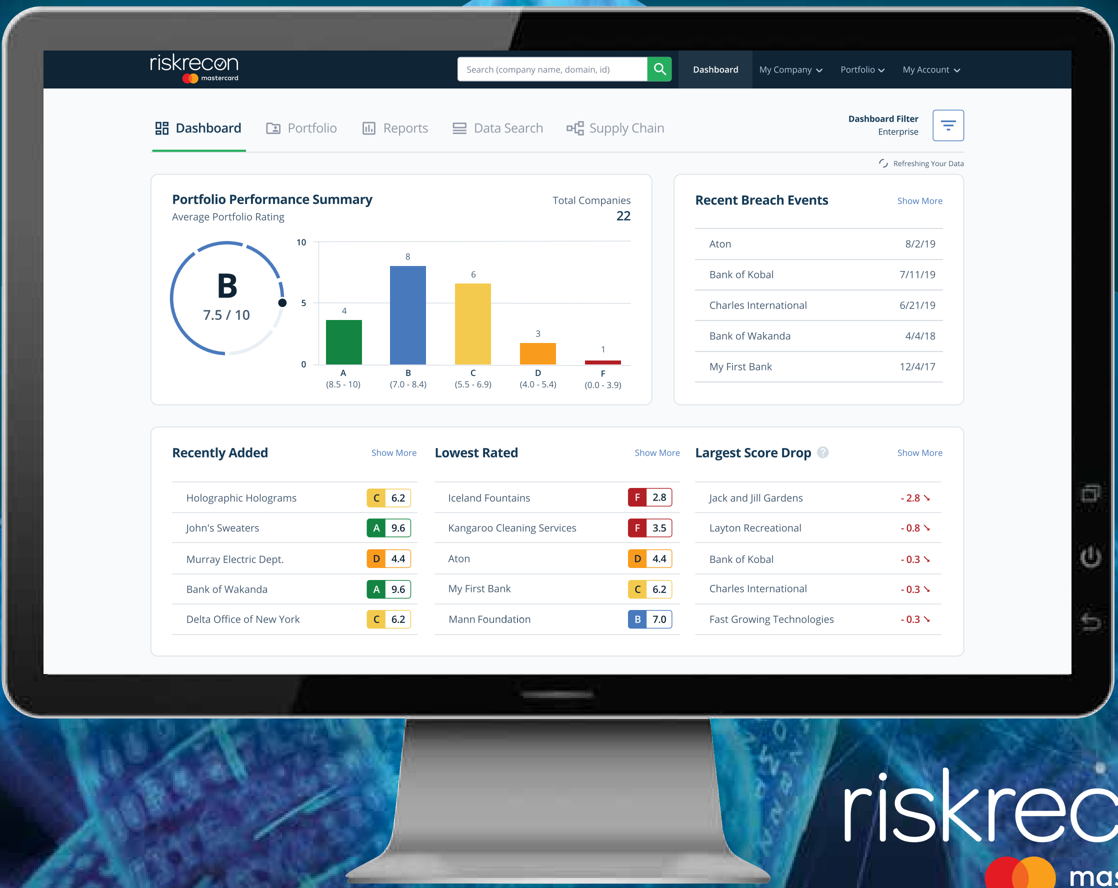
Cyber Center of Excellence	https://sdccoe.org/
FBI	
• San Diego Cyber Task Force	
• Internet Crime Complaint Center	https://www.ic3.gov/
• CyWatch	
U.S. Department of Homeland Security	StopRansomware.gov
U.S. Secret Service	https://www.secretservice.gov/
Federal Trade Commission	https://www.ftc.gov/data-breach-resources
InfraGard	https://www.infragardsd.org/
ISACA (Information Systems Audit and Control Association)	https://isaca-sd.org/
Cyber Careers & Education	https://sdccoe.org/careers/
870+ Local Cyber Firms	

Secure Your Digital Supply Chain

As a cybersecurity professional, making agile decisions with limited information is no task easy. 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



Portfolio Performance Summary

Average Portfolio Rating

Total Companies 22

Recent Breach Events

Aton	8/2/19
Bank of Kobal	7/11/19
Charles International	6/21/19
Bank of Wakanda	4/4/18
My First Bank	12/4/17

Recently Added

Holographic Holograms	C	6.2
John's Sweaters	A	9.6
Murray Electric Dept.	D	4.4
Bank of Wakanda	A	9.6
Delta Office of New York	C	6.2

Lowest Rated

Iceland Fountains	F	2.8
Kangaroo Cleaning Services	F	3.5
Aton	D	4.4
My First Bank	C	6.2
Mann Foundation	B	7.0

Largest Score Drop

Jack and Jill Gardens	- 2.8 ↘
Layton Recreational	- 0.8 ↘
Bank of Kobal	- 0.3 ↘
Charles International	- 0.3 ↘
Fast Growing Technologies	- 0.3 ↘

riskrecon
mastercard

SYSTEM
OPERATIONAL
RESERVE