SPECIAL REPORT: CYBERSECURITY

When It Comes to Facing Hackers, Preparation Is Key

Information Technology Experts Recommend Several Steps for Better Cyber Hygiene

■ BY BRAD GRAVES

A hacker infiltrating industrial computer systems and demanding a ransom forced **Colonial Pipeline** to shut down the flow of gasoline from Texas to the Northeast United States this spring.

More locally, in May, hackers demanding ransom broke into computer systems at **Scripps Health**. To contain the intrusion, IT staff shut down computer systems. The organization brought in computer experts to recover and contacted federal law enforcement. Scripps employees soldiered through the event, though access to electronic medical records was restricted, according to an account of the incident by senior management. On June 1, the organization announced its systems had been restored, but memories of the event remain fresh.

If San Diego business leaders hadn't paid attention to cybersecurity before, they are paying attention now.

"I think we're finally getting to a point where everyone realizes cyber is everyone's business," said **Lisa Easterly**, president and CEO of San Diego's **Cyber Center of Excellence**. The center is a nonprofit organization promoting regional planning, programming and best practices in cybersecurity.

Lisa Easterly
President and CEO
Cyber Center of Excellence

Many executives are wondering what to do to improve their cybersecurity and cyber hygiene.

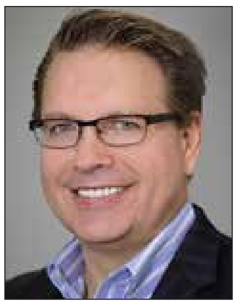
The good news is that San Diego has resources to help executives working to shore up their cyber defenses.

Indeed, the region has a robust cybersecurity community, which takes in 24,349 employees (see accompanying story). Several leaders of that community took time to share thoughts with the San Diego Business Journal about how their peers in other vertical markets might get in front of the cybersecurity challenge.

Whose Issue Is This?

"Security should not be an afterthought," said **Brad Taylor**, CEO of **Proficio**, a cybersecurity company based in Carlsbad with a worldwide footprint. "It should be designed in as part of the plan from the beginning." Also, he said, it should follow industry best practices consistently.

Company leaders need to understand that information security is a business risk issue. In other words, it's a management problem, not an information technology problem, said **Peter Bybee**, president and CEO of **Security on Demand**. The business, based in Scripps Ranch, provides cyber-threat detection services.


Peter Bybee
President and CEO
Security on Demand

Leaders of organizations "must consider cybersecurity as a strategic imperative," said **Omer Meisel**, assistant special agent in charge with the San Diego **FBI** Cyber Program.

Tony Anscombe, chief security evangelist with **ESET**, said the best way to achieve and maintain cybersecurity is to take a "pragmatic and layered approach." He recommends starting with an overall strategy — a high level plan detailing risks, assets and how they need to be protected. Just as important is a commitment to implement that plan. ESET, with its main U.S. office in Little Italy, offers software and services for IT security.

Tony Anscombe
Chief Security Evangelist
ESET

The Threat Landscape

Companies today face multiple threats, which exploit multiple vulnerabilities.

In a survey of 524 international companies, most of them with 500 employees or more, **IBM** found that the root cause of more than half of data breaches (52%) was malicious attack. Human error was the overall, root cause of 23% of data breaches while system glitches accounted for 25%.

The 2020 Cost of a Data Breach Report was researched by the **Ponemon Institute**.

Of the malicious data breaches, more than half (53%) were financially motivated, according to the research. Roughly 1 in 8 of the breaches (13%) involved nation state actors. Another 13% involved hacktivists. The remaining 12% had unknown threat actors.

In addition to hacking, the FBI lists ransomware, malware and phishing among the most prevalent cybersecurity threats. The latter involves scammers sending a message to trick a victim into giving up passwords, Social Security numbers or other valuable personal information. Businesses also face threats from insiders — people within the organization. The FBI Internet Crime Complaint center produces an annual report on the threats, available at www.ic3.gov.

The Human Element

Most cybersecurity breaches have a human in the loop, said Easterly. Therefore, any sort of cybersecurity effort can't go too far without involving an organization's workforce.

Train your staff, said **Stacey Anfuso**, president and CEO of **La Jolla Logic**. All staff with electronic system access of any type should be trained in the fundamentals of cybersecurity.

Stacey Anfuso
President and CEO
La Jolla Logic Inc.

People are a hacker's easiest access point to a system, said two representatives from **CBIZ**, which offers insurance, accounting, other business services and consulting. **Tiffany Garcia** and **Ray Gandy** said that employees must understand their roles in protecting personal and business critical data. Cybersecurity is a team effort.

"Our security consciences should be weaved into our daily activities: opening emails, paying invoices, visiting websites," said a statement from Garcia, director and national cybersecurity practice leader for CBIZ and Gandy, director and leader of the IT risk and assurance practice at CBIZ MHM.

"The most critical piece of cybersecurity is to build a culture of cybersecurity and continuously test your people, processes and technologies," said **Scott Sautter**, vice president of **Booz Allen Hamilton** and a leader at the firm's San Diego office. "Basic best practices include fostering a culture of cyber hygiene, patching regularly and training employees."

Scott Sautter
Vice President
Booz Allen Hamilton

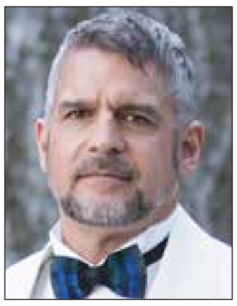
Leadership must lead by example, modeling cyber hygiene best practices, he said.

Sautter leads Booz Allen's work in network engineering, information technology infrastructure, cybersecurity, and systems engineering on the West Coast. The business is one of San Diego's larger defense contractors.

A Full-Time Effort

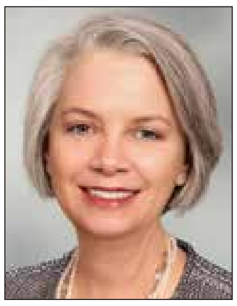
Eric Basu, CEO of **Sentek Global**, says his No. 1 cybersecurity recommendation for businesses has to do with staffing.

Name a director of security or CISO (chief information security officer) and make it a dedicated position, he said. "Too often this job is a collateral duty of the IT manager, which means the manager may allow other priorities — budget and resource constraints, technology preferences, management priorities —supersede IT security priorities."


Eric Basu
CEO
Sentek Global

Multifactor authentication for all remote access to a computer network is a must, said **Chris Reese** of **Lockton**. That includes access to email. As an insurance brokerage, Lockton does not work in cybersecurity per se, but it deals with its consequences every day.

Multifactor authentication requires a person to present two pieces of evidence — their credentials — when logging into an account. Credentials fall into any of three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). The definition comes from NIST, the **National Institute of Standards and Technology**, part of the **U.S. Department of Commerce**. Credentials must come from two different categories to enhance security — so entering two different passwords would not be considered multi-factor.


Chris Reese
Senior Vice President, Cyber and Tech Practice, Pacific Series
Lockton

Reese said that multifactor authentication is a powerful tool in addressing the cybersecurity challenges of working from home.

Basu said businesses and individuals should enable two-factor security (or 2FA) or multifactor security (MFA) on any account they don't want to have compromised. 2FA means that when logging into an account from an unknown device, a computer user will be prompted for a text message sent to their mobile device or a code provided by a synchronized application on a mobile device.

Lack of 2FA or MFA can drive a company's insurance premiums up, or can cause insurance carriers to deny coverage.

➡ *Special Report page 16*

Special Report

➡ from page 15

The Rise of Ransomware

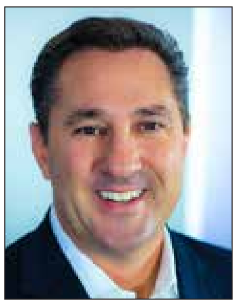
Ransomware attacks are very much in the news. Here a hacker blocks access to a company's data by encrypting it. The hacker will then offer to return the data if the victim pays a ransom.

Some observers say it is possible to get out in front of a ransomware attack, with proper detective work.

ESET's Anscombe said a ransom demand often comes some time after a hacker has first broken into a system, via a hardware or software vulnerability, or through compromised credentials (such as a stolen password).

"Ransomware attacks are now often the end phase to a broader attack," he said. "… The bad actor will map the network and gather information, identify sensitive data assets, exfiltrate the data, disable security systems where possible, and only then execute the ransomware attack." If the victim refuses to pay, the victim needs to recover the internal systems that were affected. That victim might also find stolen data published or sold on the dark web.

"The good news is that attacks don't happen immediately, so there's an opportunity to catch and prevent them," said Proficio's Taylor. "You typically have several days or even weeks to detect the bad actors before too much damage is done and most existing security products can prevent or detect these attacks — as long as you keep your security devices updated and most importantly have strong threat detection use cases, active monitoring and effective response in place."



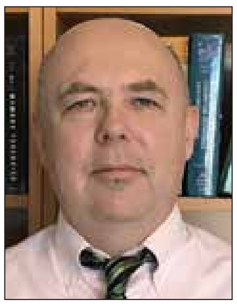
Brad Taylor
CEO
Proficio

First Steps

So, where to begin?

"The important thing is to get started," said **Chris Simpson**, director of the **National University Center for Cybersecurity**.

The nonprofit **Center for Internet Security** has a list of 18 controls that a business can implement in numerical order. "This provides a nice roadmap for a company just getting started," Simpson said. The list is available at https://www.cisecurity.org/controls/v8/.



Chris Simpson
Director
National University Center for Cybersecurity

A good early step is to build a process to securely back up data. "There are many low-cost cloud solutions," Simpson said. A company should also implement protection (that is, anti-virus/malware and firewall) on its endpoints (computers).

Lockton's Reese said another action that a person can take immediately is to rotate all passwords for business and personal accounts.

A good early step toward meeting cybersecurity challenges is to get outside help.

Cybersecurity threats are very dynamic, said Anfuso of La Jolla Logic. Therefore, engaging with outside consulting support can ensure that a business has access to the most up-to-date knowledge, skills and expertise.

San Diego is home to more than 870 cyber firms available to assist companies of all sizes and sectors with their specific cybersecurity needs, said Easterly of the Cyber Center of Excellence.

Smaller companies can consult their legal, accounting or insurance counsel for names of professionals who can help them. Other resources include economic development corporations, chambers of commerce or the Cyber Center of Excellence.

Many of the people consulted for this story recommended getting references for vendors.

"While it may be preferable that the partner has experience in your industry sector, this may not always be possible," said ESET's Anscombe.

Many companies hire a fractional Chief Information Security Officer, or CISO, and find that model affordable, said Bybee.

The Federal Perspective

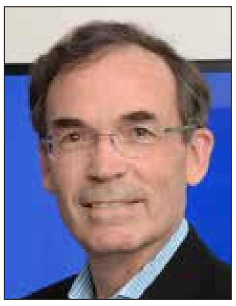
One other imperative is to establish a relationship with law enforcement, including the FBI.

Local law enforcement, the FBI and the Secret Service encourage outreach before a crisis to develop relationships, said Easterly of the Cyber Center of Excellence. The FBI's Meisel said establishing a partnership is "essential" to protecting a company's network and helping the government keep the nation secure.

Existing law puts the FBI in a unique position to collect both investigative information and intelligence regarding cyber matters, he said. "What may seem like insignificant activity to a company may be a missing puzzle piece needed to deter a larger scale intrusion/attack. Providing information to the FBI and its partners on suspicious activity occurring on company networks, may help the FBI connect the dots regarding cyber threats."

Businesses that work for the federal government, including members of San Diego's defense contracting community, have to think about federal standards when considering cybersecurity.

Two of the **U.S. Navy**'s preeminent organizations working in cybersecurity are in San Diego. They are the **Naval Information Warfare Systems Command** in Old Town (NAVWAR) and **Naval Information Warfare Systems Center** on Point Loma. They "depend heavily on local businesses for the research, development, testing and engineering" that goes into developing war-fighting capabilities, said **Mark Compton**, NAVWAR's command information security officer.



Mark Compton
NAVWAR Command Information Security Officer
U.S. Navy

Those who want to do business with the Defense Department and want to know how to protect the government's information within their non-federal information systems "should consider establishing relationships with like businesses through local chapters of defense focused associations," said Compton. "They can help you understand the government's requirements and provide recommendations on finding the right vendors to help you meet your needs."

He did not mention associations by name. However, two examples with San Diego chapters are NDIA, the **National Defense Industrial Association**, and **AFCEA International**, the Armed Forces Communications and Electronics Association.

The Work at Home Phenomenon

With the coming of the coronavirus in 2020, many people starting working at home. That caused many unsecured gaps, said Easterly.

It is critical, she said, that employees working at home use only company-issued devices with properly confirmed firewalls and anti-malware and intrusion prevention software installed. The system should not be shared with anyone else in the household.

Darren Bennett
Chief Information Security Officer
City of San Diego

"We are now operating in a new world where remote work is more commonplace," said **Darren Bennett**, chief information security officer with the San Diego city government. "You must ensure that connections from remote environments are secure and trusted." A few solutions for this, he said, are utilizing virtualization, using hard disk encryption and issuing company laptops for remote work via a virtual private network. "Also, using a virtual desktop infrastructure (VDI) can help by allowing employees to access corporate resources from almost anywhere while still controlling the exposure of the data and systems."

Remote work will remain a challenge to business, in terms of time and money. In IBM's international survey, 76% of respondents said they felt remote work would increase the time it takes to identify or contain a data breach while 70% said remote work would increase the cost of a data breach.

Taking the Temperature

Whether employees are working in the office or at home, the dynamic nature of cyber threats means businesses must continually review their cybersecurity posture.

Threats evolve, said Easterly. Therefore "cybersecurity is not a set and forget exercise."

Many of the experts consulted for this article recommend in-depth annual cybersecurity reviews. Reese, of Lockton, recommends it twice a year, then developing a roadmap on actionable items based on that review. "Prioritize the actionable items based upon their potential impact to the company," she said.

Booz Allen's Sautter said companies ought to review their cyber posture in real time ideally, and daily at a minimum.

"Staying on top of the ever-changing threat landscape mandates continuous monitoring of systems," he said. "Real time updates are critically important when working with the government. In their capability model for cybersecurity, organizations must prove they have the mandated security in order to win contracts."

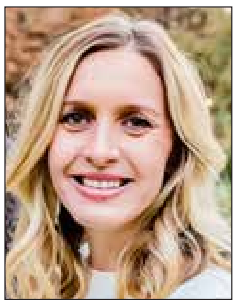
Anticipating Trouble

In the years ahead, many businesses will fall victim to a cyber breach. It is not a matter of if it will happen, but when, said the FBI's Meisel.

When a cybersecurity incident occurs, "be swift and calculated in your response," said Garcia and Gandy from CBIZ. "Every hour saved will help minimize the extent and costs associated with a security incident. Know what to do to stop the bleeding, restore operations and communicate effectively to employees, customers, authorities and others."

"There are a lot of moving parts for CIRT," Bybee said, referring to a Computer Incident Response Team. "You should get consulting services to help you get this structure in place, rather than stealing a template off the internet, and calling it done."

Easterly said a good incident response plan "should be a living document." It should offer a course of action for all significant incidents to help IT staff stop, contain, eradicate, and recover from an incident.



Tiffany Garcia
Director and National Cybersecurity Practice Leader
CBIZ

Such a plan should include an enterprise-wide risk assessment to identify and address vulnerabilities. It should name key team members and stakeholders, spelling out their responsibilities. It should include a business continuity plan. And it should list critical network and data recovery processes.

It should also contain a communications plan, considering interaction with law enforcement and the roles of legal counsel and public relations counsel.

Businesses might review the **Federal Trade Commission**'s recommendations on its website, Basu said. These can be found at https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.

An incident event log can help business leaders keep track of all steps taken during and after a cybersecurity incident, said Easterly. There are several benefits. The account will support a company's legal team and law enforcement both during and after threat detection. It can also help a company gauge the efficacy of its response and glean lessons.

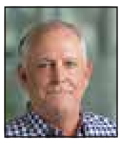
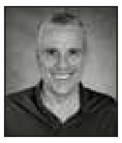
"The secret to a good incident response plan is practice," said Sautter. "There's no 'one size fits all' plan that will work for every organization. That's why it's important to regularly test and update your plan. What works today may not work a year from now, especially as technological innovation accelerates."

Given the importance of information security to the local business community, the San Diego Business Journal will host a panel discussion on best practices in cybersecurity. A recap of the event, "Understanding the Post Pandemic Cyber Threat Landscape," will be published in late July, and the event will be available for viewing on sdbj.com.

Look to the San Diego Business Journal for ongoing coverage of cybersecurity and how San Diego's cybersecurity community is responding to the challenge. ■

THE LIST CYBERSECURITY ORGANIZATIONS

Ranked by number of local full-time employees as of April 1, 2021

Rank	Company Address Website Phone	# of local full-time cybersecurity employees as of April 1, 2021	# of local-full time employees: 2021 2020 % + (-)	Products and/or services offered	Cybersecurity (Commercial/Defense)	Market Served	Top local executive Year est. locally	
1	**Naval Information Warfare Systems Command (NAVWAR)** 4301 Pacific Highway, San Diego 92110 www.navwar.navy.mil wnd	3,000	6,000 6,000 0	Naval Information Warfare Systems Command identifies, develops, delivers and sustains information warfighting capabilities and services that enable naval, joint, coalition and other national missions operating in warfighting domains from seabed to space.	Defense	International	Douglas Small 1997	
2	**Viasat, Inc.** 6155 El Camino Real, Carlsbad 92009 www.viasat.com 760-476-2200	200	2,515 2,663 (6)	Viasat's cybersecurity, data protection and information assurance solutions provide end-to-end encryption and network protection to keep classified information secure – from the edge to the cloud.	Both	Local National International	Rick Baldridge 1986	
3	**Booz Allen Hamilton Inc.** 1615 Murray Canyon Road, Suite 8000, San Diego 92108 www.boozallen.com 619-725-6500	158	1,402 1,397 0	As one of the world's largest cybersecurity solution providers, Booz Allen has defended against some of the most advanced and persistent cyber threats. For more than four decades our elite cybersecurity teams have fought at the digital frontlines	Both	Regional National International	Jennie Brooks Stephen Soules 1997	
4	**Sentek Global** 2811 Nimitz Blvd., Suite G, San Diego 92106 www.sentekglobal.com 619-543-9550	91	200 196 2	Cybersecurity, Professional Support Services, Risk Management Framework	Both	Local Statewide Regional National	Eric Basu 2001	
5	**Security On-Demand, Inc.** 12121 Scripps Summit Drive, Suite 320, San Diego 92131 https://www.securityondemand.com 858-693-5655	80	80 80 0	SOD is a Managed Security Services provider offering 24x7 Cyber-Threat Detection & Monitoring Services using Big Data analysis and advanced AI via their ThreatWatch patented subscription services.	Both	Local Statewide Regional National	Peter Bybee 2001	
6	**Proficio** 2177 Salk Ave, Suite 100 , Carlsbad 92008 www.proficio.com 800-779-5042	58	72 57 26	Proficio provides a full suite of managed security services to enable our clients to reduce risk, meet their security and compliance goals, and maximize their investments in security technology.	Commercial	Local Statewide Regional National International	Brad Taylor Tim McElwee 2010	
7	**ESET North America** 610 W. Ash St., Suite 1700, San Diego 92101 www.eset.com 619-876-5400	18	200 200 0	ESET is an internet security company that offers anti-virus and firewall products.	Commercial	Local Statewide Regional National International	Brent McCarty 1999	
8	**EVOTEK, Inc.** 6150 Lusk Blvd., Suite B204, San Diego 92121 www.evotek.com 858-362-5083	10	80 50 60	EVOTEK is unique in our ability to deliver infrastructure servides through the lens of cybersecurity. Led by former CISOs, EVOTEK delivers advisory services, programs, tools, personnel, and process.	Commercial	Local Statewide Regional National	Cesar Enciso 2014	
9	**Natural Networks, Inc.** 10225 Barnes Canyon Road, Suite A105, San Diego 92121 www.naturalnetworks.com 619-222-3232	7	10 13 (23)	We offer managed IT, phone, internet, and cloud solutions for small to medium-sized businesses.	Commercial	Local Statewide Regional National	Anthony Polselli 1994	
10	**MedCrypt** 125 S Hwy 101, Solana Beach 92075 https://www.medcrypt.com (877) 632-7978	6	6 6 0	Ghost: Cryptography Implementation Canary: Device Behavior Monitoring Heimdall: SBOM Management	Commercial	Local Statewide Regional National International	Michael Kijewski 2016	
11	**Noble Technology Group** 8139 Center St. Suite #100, La Mesa 91942 www.nobletechgroup.com 619-752-1620	5	5 2 150	CMMC Compliance for DoD Contractors.	Both	Local Statewide Regional National International	Peter Noble 2012	
12	**Innoflight LLC** 9985 Pacific Heights Blvd., Suite 250, San Diego 92121 www.innoflight.com 858-638-1580	4	64 40 60	Space software-defined radios, cryptographic/cyber-secure systems and processing avionics.	Defense	International	Jeffrey Janicik 2004	
13	**Cyber Center of Excellence (CCOE)** 610 W. Ash Street, Suite 701, San Diego 92101 https://sdccoe.org/ wnd	1	1 1 0	CCOE is a non-profit dedicated to accelerating the region's cyber economy and positioning it as a global hub of cyber innovation.	Both	Local Statewide National International	Lisa Easterly 2014	

(NR) Not ranked

Source: The companies.

To the best of our knowledge, this information is accurate as of press time. While every effort is made to ensure the accuracy and thoroughness of the list, omissions and typographical errors sometimes occur. Please send corrections or additions to the Research Department at the San Diego Business Journal. Eric Alderete, ealderete@sdbj.com. This list may not be reprinted in whole or in part without prior written permission from the editor. Some companies have declined to participate or did not return a survey by press time. It is not the intent of this list to endorse the participants or to imply a company's size or numerical rank indicates its quality.

Report Puts Cybersecurity's Economic Impact at $3.5 Billion

Sector Affects San Diego Like Nine Super Bowls or 23 Comic-Cons; Military Is a Key Driver

■ BY BRAD GRAVES

San Diego County's cybersecurity cluster is an economic giant and a growth engine.

Cybersecurity accounts for 24,349 jobs across 874 firms, and has a total economic impact of $3.5 billion annually, according to an economic study released late this month.

The new report, titled "Securing the Future: AI and San Diego's Cyber Cluster," was assembled by the **San Diego Regional Economic Development Corp.** and San Diego's **Cyber Center of Excellence**. It was underwritten by defense contractor **Booz Allen Hamilton**.

The 874 businesses mentioned are not all pure-play cybersecurity firms. The total includes firms that employ cybersecurity professionals but whose core work is something other than cybersecurity.

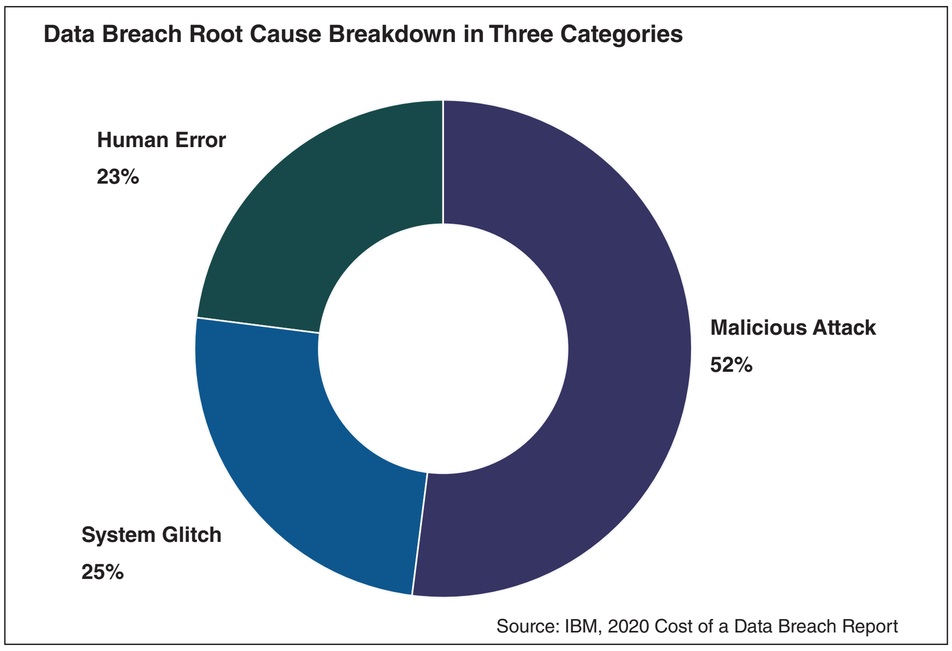
The economic impact of the cybersecurity sector is the same as nine Super Bowls or 23 Comic-Cons, report authors said. Furthermore, that impact does not stay bottled up. Each cyber job generates one more job in other industries in the region, report authors said.

Against this backdrop, San Diego companies are doing more work in the fields of artificial intelligence (AI) and machine learning. Report authors assert the trend will be good for employment, and will not take away jobs.

Employment Opportunities

Employment growth in the cyber industry has outrun that of the San Diego region as a whole.

The region's cyber employment grew 40% during the seven years since the first quarter of 2014. With the arrival of COVID-19 and the associated job losses in the general economy, total nonfarm employment in the first quarter of 2021 was roughly what it was in 2014.



Data Breach Root Cause Breakdown in Three Categories

Source: IBM, 2020 Cost of a Data Breach Report

According to the study, growth in cybersecurity continued steadily as other industries lost jobs during the first half of 2020.

Today, cybersecurity is where the jobs are. Some 61 percent of cyber businesses plan to hire workers during the next year, according to the study.

In the last 12 months, unique postings for cybersecurity jobs stood in the range of 1,400 to 1,600 per month.

Talent, however, can be hard to find. Some 80% to 90% of local cybersecurity companies interviewed said they had difficulty finding qualified workers.

Indeed, companies are looking outside the region for help. The percentage of remote positions at those companies has grown from less than 1% in the spring of 2017 to more than 9% in in the spring of 2021.

Government Contracts Abound

Nearly 3 in 5 cybersecurity firms work directly or indirectly for the federal government, including the **U.S. Department of Defense**, and 32% focus exclusively on federal contracts.

In 2020, the **Naval Information Warfare Systems Command** (or NAVWAR), the local **U.S. Navy** command focused on information technology, awarded roughly $1.6 billion in cybersecurity and artificial intelligence contracts within the San Diego region. (Overall, the command awarded a total of $7.1 billion in contracts related to cyber and AI.)

Such spending has fed the growth of San Diego's cybersecurity cluster. Report authors said that $1.6 billion is equal to 46% of the total economic contributions of San Diego's cyber cluster, "presenting an enormous growth opportunity if taken advantage of."

Artificial Intelligence on the Ascent

Much of the report covers the growth of artificial intelligence (AI) and machine learning technologies, and their role in cybersecurity.

Such technology has helped the industry, which is short on labor, by automating tedious and repeatable tasks. That has freed workers to spend their time on other pressing tasks.

Report authors assert that artificial intelligence and machine learning are creating and enhancing jobs, rather than eliminating them.

Productivity in the cybersecurity cluster has grown 7.5% since 2018, nearly triple the average for all San Diego industries. Report authors attribute that to the development and adoption of AI.

"By utilizing the vast resources at their disposal, local cyber firms can ensure continued strong growth in the years and decades ahead," the report concludes. "The need for cyber workers, products and services shows no sign of abating anytime soon, and San Diego is uniquely positioned to lead the way."

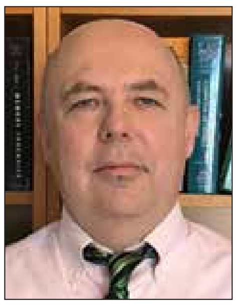
The report was funded in part by the Department of Defense. ■

Join SDBJ & CCOE for July Cyber Threat Landscape Panel

Part of Continuing Commitment to Cybersecurity Information

■ By JAY HARN

As part of its continuing commitment to informing and helping its readers understand the complexities of cybersecurity, the **San Diego Business Journal** is partnering with the **Cyber Center of Excellence** for a special cyber panel discussion that will be available to view on sdbj.com on July 26. The virtual panel will be moderated by **Lisa Easterly**, president and CEO of CCOE. The panel will focus on "Understanding the Post-Pandemic Cyber Threat Landscape." Complete coverage of the panel will also be featured in the July 26 print edition.

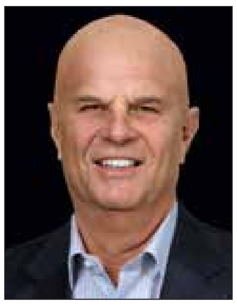


Chris Simpson
Director
National University
Center for
Cybersecurity

The CCOE is a San Diego nonprofit organization dedicated to accelerating the region's cyber economy and positioning it as a global hub of collaborative innovation.

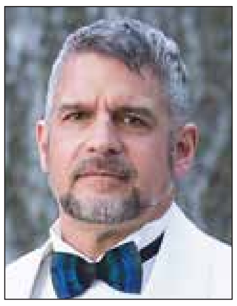
Participants

Participating in the panel discussion will be **Chris Simpson**, 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, pentesting, and incident response. He retired from the **U.S. Navy** in 2009 after 27 years of service. He holds a bachelor of science degree in computer and information science from the **University of Maryland** and a master of science degree in information security and assurance from **George Mason University**.



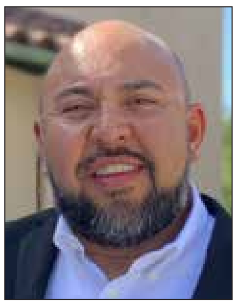
Jim Skeen Jr.
President and CEO
Lockton San Diego

Also joining the panel will be **Jim Skeen Jr**., 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 CCOE.



Eric Basu
CEO
Sentek Global

In addition, **Eric Basu**, CEO of **Sentek Global,** a technology services provider for the U.S. government mainly related to IT security program management, will be part of the panel. He is a former U.S. Navy SEAL commander who graduated from **San Jose State University** with a bachelor of science degree in molecular biology and 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 with more than 50% being veterans. He also founded the **Haiku Cyber Range**, a gamified cybersecurity simulator that teaches real world cybersecurity skills via a game interface.



Miguel Sampo
Senior Director
Riskrecon

Also joining the panel will be **Miguel Sampo**, senior director, 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. ■