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 contact 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.

“\textit{I think we’re finally getting to a point where everyone realizes cyber is everyone’s business},” said \textbf{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.

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 \textbf{Brad Taylor}, CEO of Froncio, 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 \textbf{Peter Bybee}, president and CEO of Security on Demand. The business, based in Scripps Ranch, provides cyber-threat detection services.

Leaders of organizations “must consider cybersecurity as a strategic imperative,” said \textbf{Omer Meisel}, assistant special agent in charge with the San Diego FBI Cyber Program. 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.

**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 of 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 \textbf{Stacey Antuso}, president and CEO of La Jolla Logic. All staff with electronic system access of any type should be trained in the fundamentals of cybersecurity.

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.

“Too often the 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 — to supersede IT security priorities.”

Multifactor authentication for all remote access to a computer network is a must, said \textbf{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.

“Malicious 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.”

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
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 Eyster of the Cyber Center of Excellence.

Smaller companies can consult their legal, accounting or insurance counsel for names of professionals who can help them. Others can turn to local 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.

“Law enforcement, the FBI and the Secret Service encourage outreach before a crisis to develop relationships, said Eyster 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.

Eyster added that the FBI has 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 government connect the dots regarding cyber threats.”

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

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

“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

must prove they have the mandated security in order to win contracts.”

Anticipating Trouble

In the years ahead, many businesses will be hit by a 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 Eyster.

For the record, the FBI’s Meisel said every hour saved will help minimize the extent and costs associated with a security incident. Know what to do to stop the bleeding and how to 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,” he said.

Easily 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.

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 communication 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 for doing so. This can be found at https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.

“Staying informed and being long can help business leaders keep track of all steps taken during and after a cybersecurity incident, said Eyster. 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.

“Failure to have 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 to best operate 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 sdbg.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

<table>
<thead>
<tr>
<th>Rank</th>
<th>Company Address</th>
<th>Website Phone</th>
<th># of local-full-time cybersecurity employees as of April 1, 2021</th>
<th># of local-full-time employees: 2021/2020 % (+/-)</th>
<th>Products and/or services offered</th>
<th>Cybersecurity (Commercial/Defense)</th>
<th>Top local executive</th>
<th>Year est. locally</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Naval Information Warfare Systems Command (NAVCWAR) 4301 Pacific Highway, San Diego 92110 <a href="http://www.nawar.navy.mil/wnrd">www.nawar.navy.mil/wnrd</a></td>
<td></td>
<td>3,000</td>
<td>6,000 / 6,000</td>
<td>Naval Information Warfare Systems Command identifies, develops, delivers and sustains information warfare capabilities and services that enable naval, joint, coalition, and other national missions operating in warfighting domains from seabed to space.</td>
<td>Defense</td>
<td>International</td>
<td>Douglas Small</td>
</tr>
<tr>
<td>2</td>
<td>Viasat, Inc. 6155 El Camino Real, Carlsbad 92009 <a href="http://www.viasat.com">www.viasat.com</a></td>
<td>760-476-2200</td>
<td>200</td>
<td>2,515 / (6)</td>
<td>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.</td>
<td>Both</td>
<td>Local</td>
<td>Rick Bastridge</td>
</tr>
<tr>
<td>3</td>
<td>Booz Allen Hamilton Inc. 1615 Murray Canyon Road, Suite 8000, San Diego 92108 <a href="http://www.boozallen.com">www.boozallen.com</a> 619-725-6350</td>
<td></td>
<td>158</td>
<td>1,402 / 1,397</td>
<td>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.</td>
<td>Both</td>
<td>Regional</td>
<td>Jerome Brooks</td>
</tr>
<tr>
<td>5</td>
<td>Security On-Demand, Inc. 1216 Scripps Summit Drive, Suite 320, San Diego 92131 <a href="https://www.securityondemand.com">https://www.securityondemand.com</a> 858-493-5655</td>
<td></td>
<td>80</td>
<td>89 / 0</td>
<td>SOD is a Managed Security Services provider offering 24x7 Cyber Threat Detection &amp; Monitoring Services using Big Data analysis and advanced AI via their ThreatWatch patented subscription services.</td>
<td>Both</td>
<td>Local</td>
<td>Peter Bybee</td>
</tr>
<tr>
<td>6</td>
<td>Proficio 2177 Salk Ave, Suite 100, Carlsbad 92008 <a href="http://www.proficio.com">www.proficio.com</a> 800-779-5042</td>
<td></td>
<td>58</td>
<td>72 / 26</td>
<td>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.</td>
<td>Commercial</td>
<td>Local</td>
<td>Brad Taylor</td>
</tr>
<tr>
<td>8</td>
<td>EVOTEK, Inc. 6150 Lusk Blvd., Suite B204, San Diego 92121 <a href="http://www.evotek.com">www.evotek.com</a> 858-362-5083</td>
<td></td>
<td>10</td>
<td>80 / 50</td>
<td>EVOTEK is unique in our ability to deliver infrastructure services through the lens of cybersecurity. Led by former CISOs, EVOTEK delivers advisory services, programs, tools, personnel, and process.</td>
<td>Commercial</td>
<td>Local</td>
<td>Cesar Enciso</td>
</tr>
<tr>
<td>9</td>
<td>Natural Networks, Inc. 10225 Barron Canyon Road, Suite A105, San Diego 92121 <a href="http://www.naturalenetworks.com">www.naturalenetworks.com</a> 619-222-3232</td>
<td></td>
<td>7</td>
<td>10 / (23)</td>
<td>We offer managed IT, phone, internet, and cloud solutions for small to medium-sized businesses.</td>
<td>Commercial</td>
<td>Local</td>
<td>Anthony Patsil</td>
</tr>
<tr>
<td>11</td>
<td>Noble Technology Group 6179 Center St, Suite A150, La Mesa 91942 <a href="http://www.nobletechnologygroup.com">www.nobletechnologygroup.com</a> 619-752-1620</td>
<td></td>
<td>5</td>
<td>5 / 2</td>
<td>CMAC Compliance for DoD Contractors.</td>
<td>Both</td>
<td>Local</td>
<td>Peter Noble</td>
</tr>
<tr>
<td>13</td>
<td>Cyber Center of Excellence (CCoE) 610 W. Ash Street, Suite F1, San Diego 92101 <a href="https://sdbj.com/wnrd">https://sdbj.com/wnrd</a></td>
<td></td>
<td>1</td>
<td>1 / 0</td>
<td>CCoE is a non-profit dedicated to accelerating the region’s cyber economy and positioning it as a global hub of cyber innovation.</td>
<td>Both</td>
<td>Local</td>
<td>Lisa Garofalo</td>
</tr>
</tbody>
</table>

*Not ranked

**Sources:** 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, ealdere@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 rank order the companies 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 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 cybersecurity 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 continued steadily as other industries in the region, report authors said.

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.

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.

Also joining the panel will be Jim Skeen Jr., founding president and CEO of Lockt 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 has experience in multiple strategic acquisitions and expected to have significant time and expertise to cyber risk awareness and is a founding board member of the CCOE.

In addition, Eric Basu, CEO of Sentek Global, a technology services provider for the U.S. government primarily 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 Global in 2001 and the company now employs nearly 200 individuals with more than 50% being veterans. He also founded the Hai-Ku Cyber Range, a gamified cybersecurity simulator that teaches real world cybersecurity skills via a game interface.

Miguel Sampo, senior director, global sales with Riskrecon, has more than 20 years professional cybersecurity experience working with Fortune 100-1000 organizations. He is a strategic thinker with strong technical skills married 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.

Join SDBJ & CCOE for July Cyber Threat Landscape Panel

Part of Continuing Commitment to Cybersecurity Information

**Source:** IBM, 2020 Cost of a Data Breach Report

**Data Breach Root Cause Breakdown in Three Categories**

- **Human Error:** 23%
- **System Glitch:** 25%
- **Malicious Attack:** 52%