San Diego Regional Cyber Lab

Executive Insights: Guidance for the Next Generation of Cyber Professionals

In this issue, the San Diego Regional Cyber Lab went beyond the usual updates to do something special for our community. We reached out to our Technical and Steering Committees, made up of leading CISOs, CIOs, and technical experts, to answer the kinds of questions newcomers to cybersecurity often have but may be too shy to ask. These experts come from both public and private sectors who bring deep, hands-on experience with today's most advanced technologies. Their insights ensure that every response is grounded, relevant, and directly applicable to real-world cybersecurity challenges.

At the San Diego Regional Cyber Lab, we take pride in curating our audience to ensure our resources reach those genuinely committed to growing within the cybersecurity field. Every event, training, and collaboration is designed to build meaningful connections between students, professionals, and industry leaders. We believe that growth happens when knowledge is shared openly and opportunities are made accessible to those willing to learn.

This initiative reflects our ongoing mission to close the skills gap, empower emerging talent, and foster a stronger cybersecurity community across the region. Whether through training, mentorship, or real-world experience, we remain dedicated to helping the next generation of cyber professionals build confidence, capability, and purpose.

Upcoming Events:

February 23-28, 2026
SANS Surge 2026
Marriott, La Jolla

April 4, 2026
BSides San Diego
SDSU

In This Issue

- Which questions do you wish were asked more frequently?
- What are valuable training resources for new cyber professionals?
- What is the most impressive thing you've seen in your cyber careers?
- What advice would you have liked at the start of your career?
- What are your cyber sales red flags?
- What are your favorite cyber media sources?

In our quarterly committee meetings, we asked members which security-related question they wish they were asked more frequently.

“What motivated you to get into Cybersec?”

Coworkers appreciate when others show interest in their career paths by asking questions related to their field. Asking about an experience is seen as a sign of respect and preparation. Leading to a more effective and cohesive work environment.

“How can we make cybersecurity a shared concern across all departments?”

Remind your leadership team that cyber security is everyone's responsibility. Delegating all cyber responsibilities to a single department leaves the organization highly vulnerable. A collective approach improves security by speeding up incident response. When everyone understands their role it creates a more robust and resilient culture.

What are some great training resources or organizations you recommend for people breaking into Cybersecurity?

Breaking into cybersecurity can seem daunting, but guidance from industry professionals highlights a mix of professional groups and hands-on training platforms that help newcomers build skills, gain experience, and expand their networks.

Professional Groups

- ISACA: Offers educational resources, certifications, and networking opportunities.
- CCOE: Provides free resources, work-based learning, and long-term professional networking.
- ISSA and WiCyS: Industry chapters for mentorship, peer connections, and learning opportunities.
- Meetups and Conferences: Events to connect with experts, learn emerging trends, and explore career paths.

Training Platforms

- Capture the Flag (CTF) Competitions: Hack The Box, TryHackMe, and SANS CTFs provide hands-on red and blue team experience.
- SANS Courses: In-depth training covering penetration testing, incident response, policy, and more.

What's the most impressive thing you’ve seen in cybersecurity?

During our quarterly committee meetings, we asked members to share the most impressive developments they’ve observed in the field of cybersecurity.

- One member highlighted the use of bastion hosts as an impressive yet often underestimated tool. It is a secure server—sometimes called a jump box—used to manage access to a private network from an external one. Typically exposed to the Internet, it runs minimal services to reduce its attack surface while serving as a single, secure entry point. The member noted how impressive it was to see someone use the bastion host’s command line to manage SSH and passwords efficiently.

- Another participant mentioned Stuxnet for its remarkable power and stealth. This sophisticated worm, introduced via infected USB drives, was the first to cause physical damage by targeting electro-mechanical equipment. It exploited multiple zero-day vulnerabilities, searched infected PCs for connections to control systems, and sent destructive commands. Beyond that, worms like Stuxnet can self-propagate, consume bandwidth, open backdoors, and deploy additional malware such as rootkits and ransomware.

- An expert described Scattered Spider as exceptionally bold, known for high-profile attacks and fearless social engineering tactics. Active from 2022 to 2025, the group impersonated IT support to trick employees into revealing credentials while using MFA bombing, phishing, vishing, and other evolving methods. Despite ongoing arrests, the full extent of their victims and financial impact remains unclear.

What advice and skills do cybersecurity professionals wish they had known when starting their careers?

Reflections and Advice for Starting a Career in Cybersecurity.

During our quarterly committee meetings, we asked members to reflect on their early careers in cybersecurity and share guidance they wish they had received when starting out. Their insights provide invaluable advice for anyone entering this dynamic and challenging field.

- **Foundational Knowledge:** A consistent piece of advice is understanding the fundamentals of basic networking is crucial, as it forms the backbone of modern technology and allows devices to communicate. This is foundational for any IT or cybersecurity career. Equally important is a solid understanding of science and mathematics, which supports logical thinking and rule-based decision-making, both essential for effective problem-solving in cybersecurity.

- **Engage with the Community:** Another key recommendation was to actively engage with the cybersecurity community. Joining professional chapters, attending meetups, and participating in conferences. This gives you a chance to help build a personal network, exchange insights, and develop soft skills. Being part of the community also exposes newcomers to emerging threats, industry best practices, and mentorship opportunities.

- **Gain Practical Experience:** Internships were highlighted as a crucial step for entry-level professionals. They provide hands-on experience, allowing individuals to apply technical knowledge in real-world scenarios while simultaneously developing essential soft skills. Internships also give both the student and the organization a chance to evaluate fit, making it a mutually beneficial experience.

- **Human Skills are Essential:** When asked about the most invaluable tools or skills for entry-level coworkers, participants emphasized that technical expertise alone is not enough. Human skills such as communication, collaboration, adaptability, and social awareness are equally critical. Effective communication ensures smooth workflows and clear knowledge sharing. While social awareness combined with etiquette foster strong relationships for both coworkers and clients. A willingness to learn, ask questions, and participate in community events signals dedication to one's career and commitment to the safety of others.

  Additionally, many members underscored the importance of the ability to articulate oneself. Protecting people is the core mission of cybersecurity, and technical expertise must be paired with human skills. This is necessary to navigate a complex and ever-changing environment effectively.

- **Attention to Detail:** Being detail-oriented is another non-negotiable skill. Cybersecurity professionals must operate with precision, as small oversights can escalate into significant vulnerabilities. Techniques such as verifying work, seeking a second opinion, saving copies of code or documentation, and maintaining organized notes can help prevent mistakes. As Professor Bill Reid of National University reminds us, "A copy of one is a copy of none."

In summary, for those starting a cybersecurity career, a balanced approach is essential: combine technical knowledge with practical experience, actively engage with the community, hone human skills, and maintain meticulous attention to detail. We hope this guidance equips newcomers to enter the field confidently to succeed in protecting the systems and people that depend on them.

What are some Cybersec sales red flags that are important to look out for?

- **Fear Mongering**: Sales pitches that are designed to scare their audience by focusing on breaches and their potential consequences can be overwhelming and misleading, often pressuring companies into unnecessary purchases without assessing their true needs.
- **Offering Extra Tools**: Vendors may promote additional products to justify high costs, even when they are not required. Always request a free trial or demo to evaluate the product's actual value.
- **AI Hype**: Claims such as "AI makes us the best" are oversimplified and can be misleading. Concrete examples and real-world results should support any AI-related claims.
- **Buzzword Overload**: Terms like "Next Gen", "Unhackable," or "Perpetual/ Lifetime Licenses" can misrepresent a product's capabilities or longevity if not supported by data, potentially creating confusion and misaligned expectations.

By recognizing these red flags, organizations and individuals can make more informed decisions, avoid unnecessary spending, and ensure the tools they adopt truly strengthen their cybersecurity posture.

The 2025 San Diego Cybersecurity Stewardship Awards Winners

The San Diego Regional Cyber Lab has been recognized for its leadership in promoting cybersecurity awareness and protection throughout the region. This year, our lab equipped small and micro businesses with ESET Ultimate Protection plans. Packages featuring antivirus, anti-phishing, and firewall defenses with a three year guarantee for up to five devices. These efforts help local organizations strengthen their digital resilience, safeguard sensitive data, and maintain business continuity in an evolving threat landscape.

The lab also launched My eCISO, a chatbot built on the NIST Cybersecurity Framework that guides users through self-assessments and offers tailored recommendations to improve their security posture. This innovative tool bridges the gap between awareness and implementation, making cybersecurity planning more accessible and actionable for businesses of all sizes.

What types of cyber-related media do you consume in your personal time?

Podcasts

- Dark Reading
- Palo Alto
- Cyber Wire Daily
- CISO Tradecraft

Cyber News

- Security Week
- CSO Online
- Cyber Wire Daily
- CISO Tradecraft

Additional cyber media content and resources can be found on our website here.

Connect With Us

Contact Us

SDRCL Program Lead
Ian Brazill
IBrazill@sandiego.gov

SDRCL Cyber Lead
Brendan Daly
BMDaly@sandiego.gov

Cyber Center of Excellence (CCOE), Community Partner
Lisa Easterly
Lisa.easterly@sdccoe.org

San Diego Regional Cyber Lab
1200 Third Avenue, Suite 1800
San Diego, CA 92101
http://www.sandiego.gov/cyber-lab

SAN DIEGO REGIONAL CYBER LAB