

San Diego Regional Cyber Lab



Prepping for Launch!

The launch of the new San Diego Regional Cyber Lab is just around the corner — and we can't wait to show it off!

Right now we're busy building out the physical lab space, developing virtual cyber ranges, creating a new website, and more! We're crafting this Cyber Lab to be an effective and productive resource for the entire San Diego region as we work together to make each other stronger in the defense against rising cybersecurity threats.

We'll keep you posted about when the Cyber Lab will officially open its doors, and make sure you're invited to see it for yourself.

The Cyber Lab will be sharing critical, real-time information about the latest threats and industry trends — so why wait?

This new quarterly newsletter will provide you updates on our progress and share tips, resources and other valuable information.

As a regional IT resource, this is your newsletter too. Have a problem you can't solve? Got a suggestion to make the Cyber Lab even better? How about an interesting article/podcast to share? Let us know.

We also want to share your stories. Holding a local computer security competition? What knowledge can you share? We're all ears.

This newsletter is a starting point — and with your help — can become a valuable resource for our region, especially for your less tech-savvy employees. We'll keep things simple and straightforward, and leave the jargon at home (or at least we'll try).

Thank you for supporting the San Diego Regional Cyber Lab!

Upcoming Events

- [SDRCL Website Release](#)
- [SDRCL Physical Lab Equipment Installation](#)
- [SDRCL Physical Lab Showing & Walkthrough](#)

In This Issue

- Prepping for Launch!
- New Cyber Lab Website!
- Let's Get Physical
- Cybersecurity Tips
- Did You Know?
- Latest Cyber News
- Let's Get Together (And Feel Alright)
- Kids These Days...
- By the Numbers

New Cyber Lab Website!

We're slapping a lot of 1s and 0s together to create a dynamic website for the Cyber Lab that will have a plethora of information and resources for you to explore. Those include:

- Calendar to book time in the physical lab
- Compilation of key IT resources in the San Diego region
- Cyber threat intelligence feeds
- Access to our internal Base Camp site — provides additional collaborative workspaces for agencies to share sensitive files, cyber threat data, and more.
- Information about Free Cyber Range
- Tips & best practices from industry leaders
- Compilation of the best cybersecurity-related resources (podcasts, newsletters, etc.)

Let's Get Physical

Life is hard. It gets even harder when you don't have the right tools to fend off a cyberattack. That's why we're equipping the Cyber Lab with top-notch hardware and equipment to get the job done.

The lab will be housed at the Civic Center Plaza in downtown San Diego, and here's what you'll find inside:

- Five Operations stations with MacBook Pros
- Multiple rack servers with a security gateway
- Forensic imaging tools
- Forensic duplicator
- Associated forensics software licenses (e.g. Cellebrite)
- And more!!

Cybersecurity Tips

Enterprise Level Company:

- Utilize penetration testers to identify weaknesses in your environment
- Create an Incident Response Plan, practice it annually with your management team
- Utilize phishing simulations to test employee knowledge

Mid-Size Company:

- Train your staff on cybersecurity principles
- Create a mobile device action plan. How are you maintaining security on those devices?
- Employ best practices for any card payment transactions
- Do not neglect your security budget to save a few dollars

Small/Startup Company:

- Always incorporate two-factor authentications (2FA) when possible
- Backup your data! Cloud storage makes this as easy as ever
- Stay up to date with all software/security patches

Did You Know?

Other major U.S. cities have implemented similar “Cyber Lab” services for their regions, including New York and Los Angeles. Efforts to have a decentralized, collaborative workspace that blends public and private institutions is widely considered the future of the IT industry.

We hope that with your cooperation and support, the success of the San Diego Regional Cyber Lab will be a model for other regions to follow.

Together, we can combat the major security hurdles of the day, and better prepare ourselves for the problems of tomorrow.

Latest Cyber News

Cybersecurity news changes by the minute, so you have to keep pace by staying informed on the latest threats and industry trends. Here are a few recent articles that we consider a must-read:

Ransomware anatomy: Dual cyberattacks on provider call for vulnerability review:

A recent instance of two simultaneous cyberattacks on a Canadian healthcare provider displays the latest risks associated with a lack of rapid patching of organizational vulnerabilities. More info [here](#).

7 Steps to Take Right Now to Prepare for Cyberattacks by Russia:

Here are seven recommended security measures that experts say you should already have in place within your organization. Review them to ensure you are as safe as possible during the current international conflict. More info [here](#).

How AI Is Shaping the Cybersecurity Arms Race:

Artificial Intelligence is being leveraged today as one of the newest sources of both cyberattacks and cyber defenses. Your organization should familiarize themselves with both sides of this arms race. More info [here](#).

Let's Get Together (and Feel All Right)

We know you're all eagerly anticipating the return of in-person events, so here's a few to put on your radar this year:

- **May 5-10 - SANS Security West 2022 (San Diego, CA)**. Learn hands-on cybersecurity skills at this highly technical training event. More info [here](#).
- **October 10-12 - Techno Security and Digital Forensics Conference (San Diego, CA)**. Provides an educational experience that blends the digital forensics and cybersecurity industries for collaboration between government and private sectors. More info [here](#).
- **August 6-14 - Blackhat & DEF CON (Las Vegas, NV)**. Attend briefings, trainings, and live competitions with fellow cybersecurity experts and novices alike to help ensure your organization stays up to speed on all things cybersecurity. Blackhat info [here](#). DEF CON info [here](#).

Kids These Days ...

Having trouble keeping up with the latest IT lingo? Here are a few terms that you and your team should be aware of:

- **Black hat/White hat** - Hackers that violate computer security for personal gain or malice (Black hat), or hackers that perform penetration testing on behalf of an organization to bolster their cyber posture (White hat).
- **Botnet** - A collection of computers compromised by malicious code and controlled across a network
- **Capture the Flag (CTF)** - Competition in which “flags” are purposefully hidden in vulnerable programs or websites for cyber enthusiasts to locate and retrieve before their opponents do.
- **Clickjacking** - Also known as a user interface redress attack, this is a common hacking technique in which an attacker creates an invisible page or an HTML element that overlays the legitimate page.
- **Log4j** - Java-based logging utility which records errors and routine system operations and communicates diagnostic messages back to SysAdmins. Recently found to be associated with a significantly harmful vulnerability.
- **Smishing** - Any kind of phishing that involves a text message.
- **Zero-Day** - A recently discovered vulnerability that hackers often utilize to attack systems.

SAN DIEGO
REGIONAL
CYBER LAB



San Diego Regional Cyber Lab

1200 Third Avenue
San Diego, CA 92101

By the Numbers

\$6 Trillion

Approximate damages from cybercrime in 2021.
([Source](#))

300%

Increase of attacks on Internet of Things (IoT) devices in 2019 ([Source](#))

30%

Projection of year-over-year growth in damage costs caused by ransomware over the next 10 years ([Source](#))

Contact Us

SDRCL Program Lead
Ian Brazill
IBrazill@sandiego.gov

SDRCL Cyber Lead
Brendan Daly
BMDaly@sandiego.gov

Chief Information Security Officer, CoSD
Darren Bennett
DBennett@sandiego.gov

SDRCL Project Manager
Megan Hartung
MHartung@sandiego.gov

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