San Diego Regional Cyber Lab

Hello World... The Cyber Lab is LIVE!

It is with great pleasure that we are finally able to announce that the Cyber Lab is now live! Our doors are open and future plans for lab events are underway. From collaborations with local academia, to free cybersecurity software licenses, to regional training sessions, there are many reasons to be excited about the future. In the past month, the San Diego Regional Cyber Lab's working group met with stakeholders in a regional kick-off call, met with the local ISACA San Diego group to discuss the lab's regional capabilities, and gathered informative feedback through a brand new regional survey. If you attended either of our recent local presentations, we are very thankful for your participation and willingness to explore the exciting new possibilities our lab has to offer.

We'd like to provide you with a few statistics gathered from our recent regional survey. It is important to disclose this data as we believe this will further underline why it is critical that we continue to work together to improve our regional resiliency.

- Respondents represented a wide array of agencies, including **municipal governments**, **education**, **private industry**, and **special districts**.
- **64%** of respondents have one or less dedicated cybersecurity employees.
- Respondents' top three most concerning cyber threats/attacks are **ransomware**, **phishing**, and **vulnerability exploitation.**
- The areas of respondents' organizations that they were most concerned about being targeted were **Human Resources**, **finance**, and **management**.
- **64%** of respondents do NOT perform regular penetration testing.
- The three biggest challenges to improving cyber security in respondents' agencies were **budget**, **staffing expertise**, and **training**.

Upcoming Events:

- *San Diego Cybersecurity Awareness Program (3/2)*
- *San Diego Cyber Security Summit (3/3)*
- *Regional Cyber Lab Workshop w/ Cal Poly SLO (3/13)*

In This Issue

San Diego Cybersecurity Awareness Program

The City of San Diego is inviting local small businesses to participate in the San Diego Cybersecurity Awareness Program. The City is partnering with the Cyber Center of Excellence (CCOE) to help small businesses increase their cybersecurity awareness and preparedness to bolster the region's economic resiliency. The program is **FREE** to participating small businesses, made possible by a grant from the City of San Diego.

Offerings include:

- Detailed cybersecurity risk assessment from MasterCard's RiskRecon.
- Cybersecurity awareness training for up to 100 employees from ESET.
- Tools to develop and exercise your cyber incident response plan with CyberCatch's simulator.
- Threat landscape briefing from the FBI.
- Connectivity to the region's cybersecurity industry including additional customizable resources.

Click here to RSVP for the informational webinar on **March 2nd at 10am**. If you wish to register for additional complimentary cybersecurity offerings, click here.

**Note: To be eligible to participate, you must have 100 or fewer employees and be a San Diego business located in the City of San Diego.*

CyberCatch – Cyber Resiliency is Key and the Key to Cyber Resiliency is Incident Response

By CyberCatch

It is not a question of IF, but WHEN your organization will have an incident. The threat actors will attempt to break into your network to steal data and install ransomware. How you respond and when you respond will be the difference between minimizing damage and even thwarting the attackers or falling victim and suffering significant financial, operational and reputational harm.

An Incident Response Plan and a simulation of an incident to test the plan is the key to success.

CyberCatch's Cyber Incident Simulator is a terrific tool currently being offered by the San Diego Regional Cyber Lab. The City of San Diego itself has used this tool to enhance cyber resiliency at various City departments. Now that the San Diego Regional Cyber Lab has made licenses available for its regional partners, you too can enhance your cyber resiliency, Your success is San Diego's success, as we are all one community.

The Cyber Incident Simulator is an online virtual tool that you can use with your incident response team to test your cyber resiliency and in less than 90 minutes you will know where your gaps and blind spots are and what you need to do to be better prepared to handle an incident such as a ransomware attack.

Here is a 2-minute demo of the Cyber Incident Simulator.

Once you watch the demo, you can submit a request to the San Diego Regional Cyber Lab for a complimentary license for your own business. Click here to locate our request form, near the bottom of the page.

K-12 Cybersecurity Report: 2021-2022 School Year *(MS-ISAC, CIS)*

Top security concerns to K-12 Institutions:

- Lack of sufficient funding
- Increasing sophistication of threats
- Lack of documented processes
- Lack of a cybersecurity strategy
- Inadequate availability of cybersecurity professionals

Additional details regarding the security threats above:

- The average K-12 school allocated 8% or less of their IT budget for cybersecurity
- 29% of K-12 MS-ISAC member organizations reported being victims of a cyber incident
- 37% of K-12 MS-ISAC members do not have an incident response plan
- 49% of K-12 schools have between one and five cyber/IT employees
- 81% of K-12 MS-ISAC members have not fully implemented Multi-Factor Authentication (MFA)

2022 Cyber Recap & Future Cyber Trends *(Cal-CSIC)*

- Ransomware affected 14 of 16 critical infrastructure sectors (CISA)
- 38% increase in cyberattacks in 2022
- Over 769k cybersecurity job openings as of September 2022
- By the end of 2023, 75% of world govts. will have some form of data privacy laws
- New social engineering threats in 2023: Deep Fakes and AI technology
- Risk increasing for small and mid-sized businesses

Top exploited Vulnerabilities in 2022:

- Log4Shell
- Follina
- Spring4Shell
- Google Chrome Zero-Day

Bolstering Your Cybersecurity Posture

By Brendan Daly, City of San Diego

Developing a cybersecurity awareness program doesn't need to be costly or complicated. By adopting these fundamental concepts any organization can develop and mature their cybersecurity posture and awareness program over time.

1. **Executive Buy-In:** Gaining leadership support is important to the success of a cybersecurity awareness program at any sized organization. Effective cybersecurity is holistic and includes communicating that sound cybersecurity practices are directly linked to the success of any organization's goals and mission. Demonstrate to leadership how technology plays a critical role in all aspects of your organization and how a compromise to this technology could directly or indirectly impact operations and services. The benefits of gaining leadership support are two-fold: Increase your cybersecurity posture by bringing awareness of its importance to top level executives and this top level understanding will make it much easier for you to implement cybersecurity policies and procedures as your agency matures.

2. **Perform Vulnerability Assessments:** Vulnerability assessments can vary in scope from very lengthy and complex to simple and self-assessed. The point being that you don't know your exposure to risk unless you regularly evaluate it. Regularly evaluate your organization's exposure to vulnerabilities and its security posture to identify areas for improvement and report these findings to your leadership. Through our partnerships with local academia the SDRCL offers free vulnerability assessments to regional entities. We also provide information on resources for guided and assisted self-assessment offerings through the Center for Internet Security (CIS) and the Cybersecurity & Infrastructure Security Agency (CISA) on our resources page.

3. **Provide Training:** Providing effective cyber awareness training to all employees, both IT and non-IT, is foundational to any cybersecurity awareness program. While there are many great commercial products available for this, the SDRCL provides information on free training resources applicable to both IT and non-IT staff to get you started. See our resources page and check back often as content will be added regularly.

4. **Perform Simulated Tabletop Exercises:** A tabletop exercise is a discussion-based activity where team members discuss roles, procedures and plan execution during a simulated cybersecurity incident. Including members from all roles in the organization is great way to raise the overall cyber awareness of your organization. The SDRCL is providing free licenses for CyberCatch, a virtual tabletop exercise cyber incident simulator, for use by regional organizations. Use our Request Form to request a license for your organization.

5. **Track Results and Improve:** Track the training results of your users and tabletop exercises over time. CyberCatch in particular provides a dashboard for tracking the progress of your organization as you compete exercises. Tracking results allows you to build risk profiles for users and groups in your organization and develop more targeted trainings over time.

6. **Implement and Improve Policy:** It's crucial to implement organizational policies around cybersecurity. Utilize the training and exercises listed above to emphasize cybersecurity policy to all users in your organization and observe how existing policies may need to be adjusted or improved. Don't have cybersecurity policies or have polices that have not been updated in a long time? No problem – the SDRCL offers plenty of policy templates, best practices and resources to assist you.

Spotlight: CyberStart America

If you've visited our cybersecurity resources tab on the SDRCL website over the past month, you may have noticed one of our newest additions. On our site you will find a link to CyberStart America, a new program dedicated to giving High School students in the US access to cybersecurity learning resources developed by industry professionals. Students in this age range can apply online to receive a FREE license for CyberStart, a gameified learning space which guides students through a series of interactive game-like puzzles and tasks to learn the basics of cybersecurity.

Students can crack codes, find flags, and more as they build up their repertoire of cyber skills. Depending on how far they make it in the game, they could also be eligible for scholarship opportunities through the National Cyber Scholarship Foundation. On April 6th, the top players of CyberStart will be invited to apply for this scholarship and will be given two weeks to apply.

The following are specific offerings within CyberStart :

- Tackle **four unique bases**, each focusing on both offensive and defensive cybersecurity disciplines.
- Explore over **200 unique security challenges** which you'll solve as a cybersecurity agent investigating criminal gangs.
- Get access to an **extensive field manual** featuring video demos, top tips and essential background information to help with challenges.
- Unlock a hidden interest, progress from novice to expert and demonstrate your skills to **win scholarships**.

Royal Ransomware Attacks on the Rise

Attacks by the Royal Ransomware gang increased drastically over the course of 2022, especially for the healthcare industry. If this is the first you're hearing about them, let us provide you with a brief overview of the threat and how to best protect yourselves.

Reports state that Royal pays for Google ads to appear as top results for users, mimicking legitimate websites like food delivery services. After navigating the fake site, users are provided with fake subscription renewal emails and are encouraged to call their "company." Agents then use social engineering tactics to take control of the user's computer and gain access to corporate networks. Files are then installed on the computer and the ransomware attacks begin, so far ranging in costs between $250,000 and $60 million.

Researchers have cited the following actions for protecting yourselves from these attacks:

- Enable Microsoft Defender for Office 365 to guard against phishing by inspecting the body of emails and URLs for patterns.
- Leverage mail flow rules and capture suspicious keywords or review broad exceptions, such as those related to domain-level "allow lists" and "IP ranges" to prevent Royal from abusing legitimate services.
- Enable Safe Links for Microsoft Teams, emails, and Office applications.
- Provide user awareness training regarding email threats and social engineering.

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

No-Cost Student Assistance Available Now

If your organization has had any difficulties affording independent third party vulnerability assessments of your infrastructure, this message is for you.

The SDRCL has partnered with local universities to pair senior-level cybersecurity students with regional agencies to conduct projects specific to your own needs.

Along with vulnerability assessments, these students can similarly provide a wide array of other cyber services, including policy development and cybersecurity consulting. Contact us now if you are interested in this opportunity!

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

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