Presenters

Darren Bennett
Chief Information Security Officer
City of San Diego

Ian Brazill
Program Manager
City of San Diego

SAN DIEGO REGIONAL CYBER LAB
AGENDA

- Regional Needs / Survey Results
- Cyber Lab Mission & Vision
- Resources and Tools
- Local Collaborations
- New Opportunities
- Q & A
Cybersecurity in 2023

Global Cost of Cyber Crime (Compared to World Economies):

1. United States
2. China
3. Cybercrime
4. Japan
5. Germany

• The average cost of a data breach in 2020 was $3.86 million. (IBM security)

• The average time to identify a breach in 2020 was 207 days. (IBM security)

• About 77% of organizations do not have an incident response plan. (Cybint)

• Remote workers have caused a security breach in 20% of organizations. (Malwarebytes)
Examples of Local Cyber Threats

- San Diego Unified School District
- Scripps Health
- UC San Diego Health
- Port of San Diego
- Other: What events didn’t make the news?
2020 Survey Results

How many employees are dedicated to cyber security?

- 1 staff member: 31%
- 2 staff members: 5%
- 3 staff members: 3%
- 5 or more: 8%
- None, Cyber is a collateral duty: 53%

Does your agency conduct consistent cyber security training or exercises?

- Yes: 47%
- No: 44%
- Not consistently: 6%
- I don’t know: 3%
2020 Survey Results

If the region had a cyber center with a free cyber range or tools, would you use it?

- Yes: 92%
- No: 8%

If free or low-cost technical cyber response training was available, would you/your staff attend?

- Yes: 97%
- Yes, not sure about other staff: 3%

Would you be interested in a secure library system for templates, best practices, after action reports, etc.?

- Yes: 92%
- No: 8%
MISSION
To provide the greater San Diego region with coordinated cybersecurity awareness through collaborative access to tools, intelligence, and a trained and capable workforce.

VISION
To enhance cyber security resilience within the San Diego region through timely sharing of unclassified information, analytic products, and products for cyber security professionals.
STAKEHOLDERS
REGIONAL SUPPORT

- Information Sharing Environment
- Cyber Range
- Tools Library & Training
- Website
Workspace:
- 5 PCs and 5 Macs and dual monitors

Infrastructure:
- Dedicated secure network w/ high bandwidth
- Server rack w/ 3x DL380s, firewall, and network switch

Forensics Hardware:
- Tableau TD2U/TX1 units
- Writeblockers
- Cellebrite UFED Touch2 Ultimate
- Smart phones (iOS and Android)

Forensics Software:
- OpenText EnCase Forensic & SMS
- Oxygen Forensic Detective

Other Software:
- Recorded Future
- CyberCatch
- World of Haiku & Haiku Pro
- AWS Virtual (Free) Range
CYBER RANGES

• Two safe sandbox environments to simulate cyber attacks AND defenses
  - On-site & AWS ranges

• Video-game style range for beginners with Haiku

• Allows organizations to test their personnel’s cyber security skills

• Simulate critical infrastructure targeting
WEBSITE

SAN DIEGO REGIONAL CYBER LAB

HOME • CYBER HUB • RESOURCES • EVENTS

Stay Secure, San Diego

The San Diego Regional Cyber Lab’s mission is to provide the greater San Diego region with coordinated cybersecurity awareness through collaborative access to tools, intelligence, and a

https://www.sandiego.gov/cyber-lab
COLLABORATIVE ENVIRONMENT

- Web-based library
- Secure forum-like features
- General cyber information and specific resources by organization type
- Local cyber calendar
- Regional collaborative platform workshop session with Cal Poly
<table>
<thead>
<tr>
<th>ACADEMIA</th>
<th>PRIVATE SECTOR</th>
<th>PUBLIC SECTOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Hands-on experience with real cyber forensics tools</td>
<td>- Templates for cybersecurity policy development</td>
<td>- Cybersecurity governance, technical expertise, and guidance</td>
</tr>
<tr>
<td>- Cybersecurity training opportunities</td>
<td>- Emergency Operations Plan, Incident Response Plan, etc.</td>
<td>- Assessment of vulnerabilities and systems resilience</td>
</tr>
<tr>
<td>- Collaboration opportunities with local academic institutions</td>
<td>- Cyber training opportunities for underdeveloped IT staff</td>
<td>- Information about latest regional cyber attacks</td>
</tr>
<tr>
<td>- Develop local industry connections &amp; hiring opportunities</td>
<td>- Networking with other local public/private agencies</td>
<td>- Testing current offensive/defensive capabilities in a safe sandbox environment</td>
</tr>
<tr>
<td>- Easily accessible no-cost physical space for class activities</td>
<td>- Testing current offensive/defensive capabilities in a safe sandbox environment</td>
<td>- Cyber training for staff lacking in cybersecurity expertise</td>
</tr>
</tbody>
</table>
Thank you
Contacts:
Darren Bennett: DBennett@sandiego.gov
Ian Brazill: IBrazill@sandiego.gov