SAN DIEGO REGIONAL CYBER LAB

ISACA San Diego Chapter Meeting

January 19, 2023

Presenters

Darren Bennett

Chief Information Security Officer

City of San Diego

Ian Brazill

Program Manager

City of San Diego

SAN DIEGO REGIONAL CYBER LAB

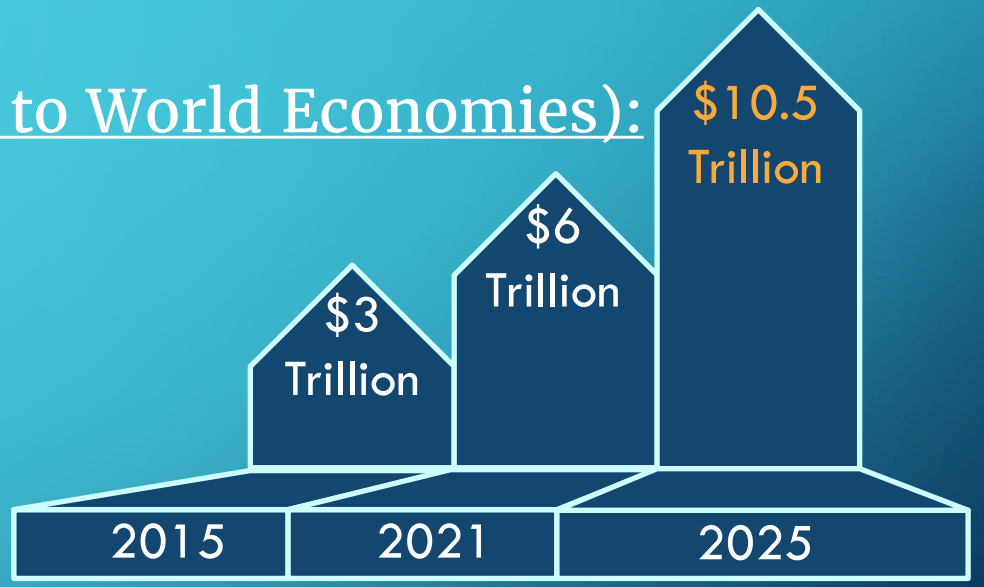
AGENDA

- 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



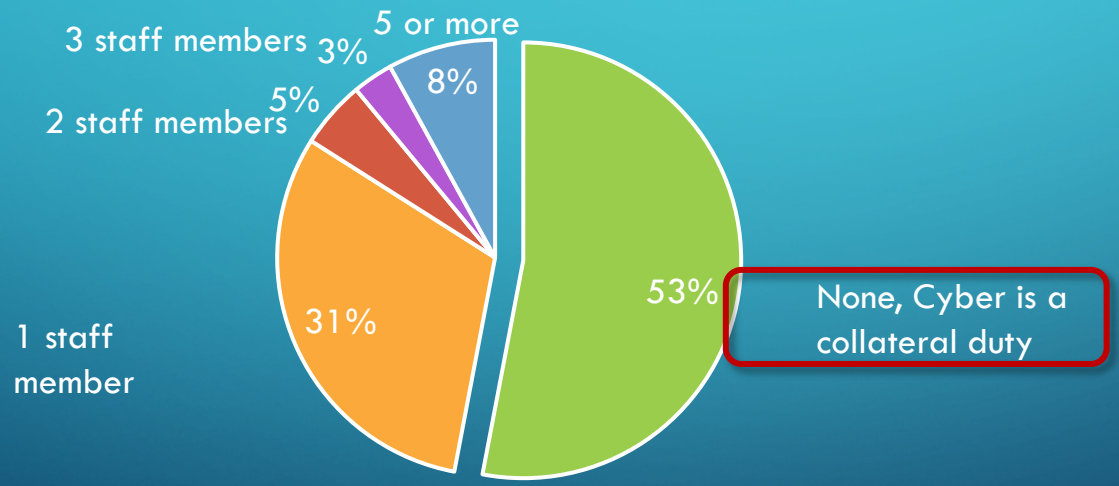
- The average cost of a data breach in 2020 was $3.86 million. *(IBM security)*
- The average time to identify a breach in 2020 was 207 days. *(IBM security)*
- About 77% of organizations do not have an incident response plan. *(Cybint)*
- Remote workers have caused a security breach in 20% of organizations. *(Malwarebytes)*

Examples of Local Cyber Threats

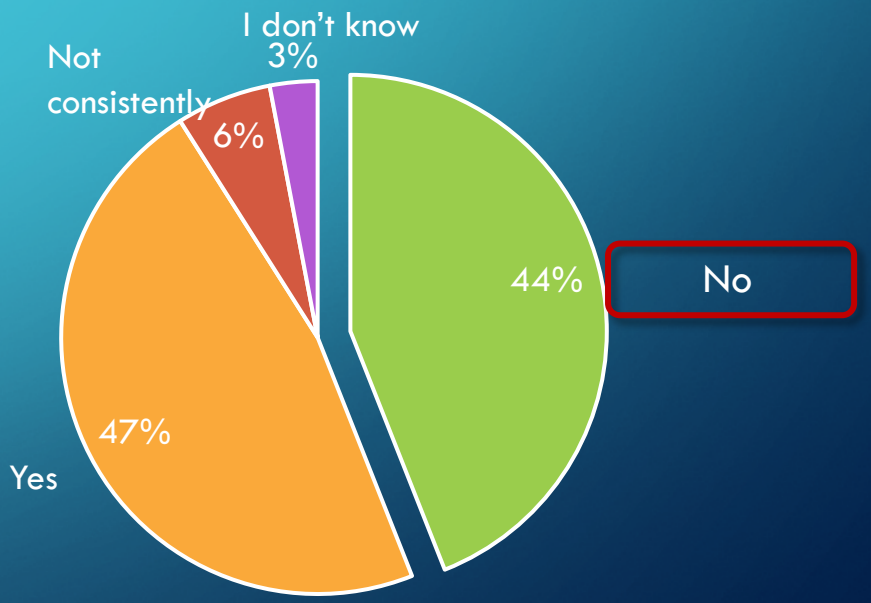
- San Diego Unified School District
- Scripps Health
- UC San Diego Health
- Port of San Diego
- Other: What events didn't make the news?

2020 Survey Results

How many employees are dedicated to cyber security?

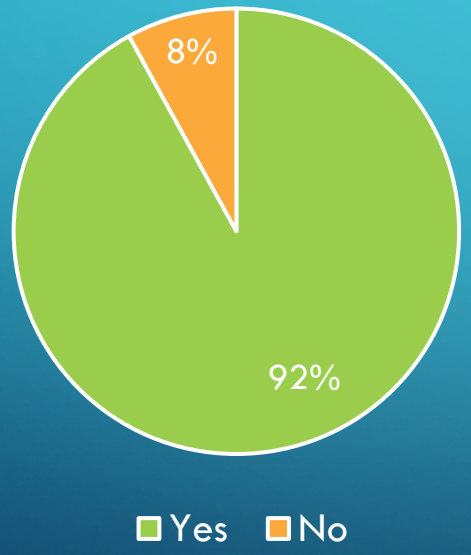


Does your agency conduct consistent cyber security training or exercises?

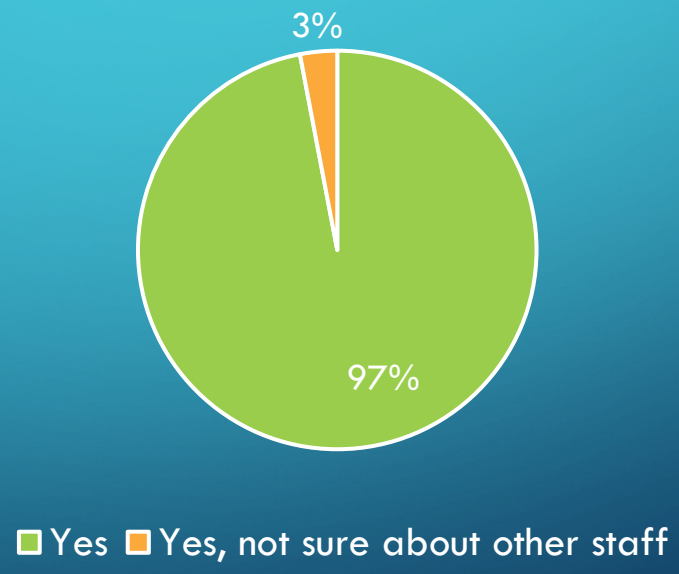


2020 Survey Results

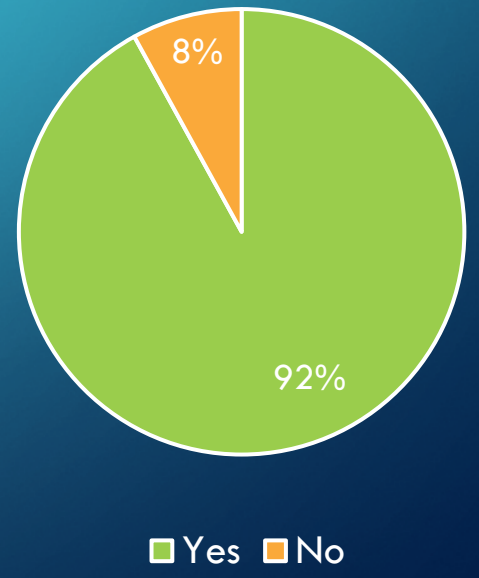
If the region had a cyber center with a free cyber range or tools, would you use it?



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



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



SAN DIEGO REGIONAL CYBER LAB

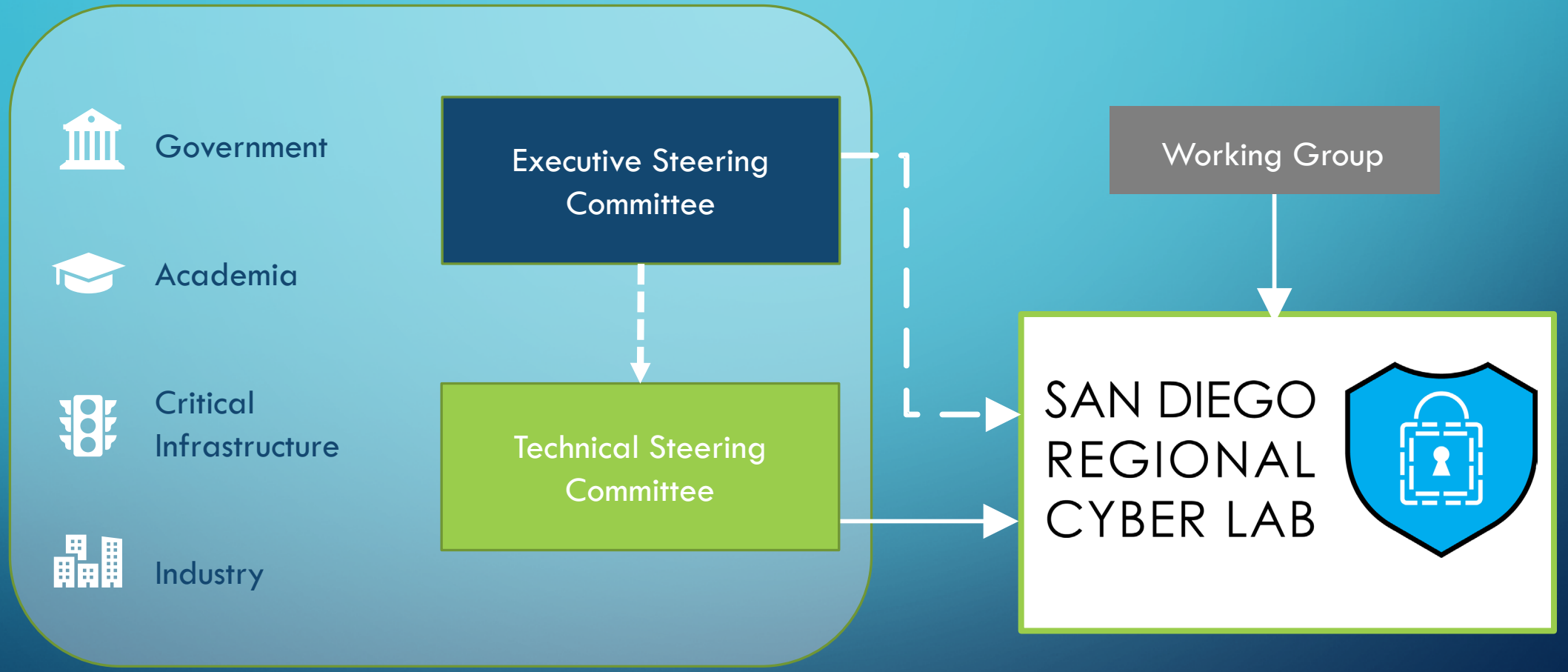
MISSION

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

RESOURCES

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

[Hai:ku]
CYBER RANGE

- 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

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

ACADEMIA

- Hands-on experience with real cyber forensics tools
- Cybersecurity training opportunities
- Collaboration opportunities with local academic institutions
- Develop local industry connections & hiring opportunities
- Easily accessible no-cost physical space for class activities

PRIVATE SECTOR

- Templates for cybersecurity policy development
  - Emergency Operations Plan, Incident Response Plan, etc.
- Cyber training opportunities for underdeveloped IT staff
- Networking with other local public/private agencies
- Testing current offensive/defensive capabilities in a safe sandbox environment

PUBLIC SECTOR

- Cybersecurity governance, technical expertise, and guidance
- Assessment of vulnerabilities and systems resilience
- Information about latest regional cyber attacks
- Testing current offensive/defensive capabilities in a safe sandbox environment
- Cyber training for staff lacking in cybersecurity expertise

Thank you

Q & A

Contacts:
Darren Bennett: DBennett@sandiego.gov
Ian Brazill: IBrazill@sandiego.gov