



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY PROGRAM (SC CIC)

Caitlin Scroggins
SC CIC Program Coordinator

AGENDA



- CYBERSECURITY AND WHY IT MATTERS
- CYBER CRIME BY THE NUMBERS
- SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY PROGRAM

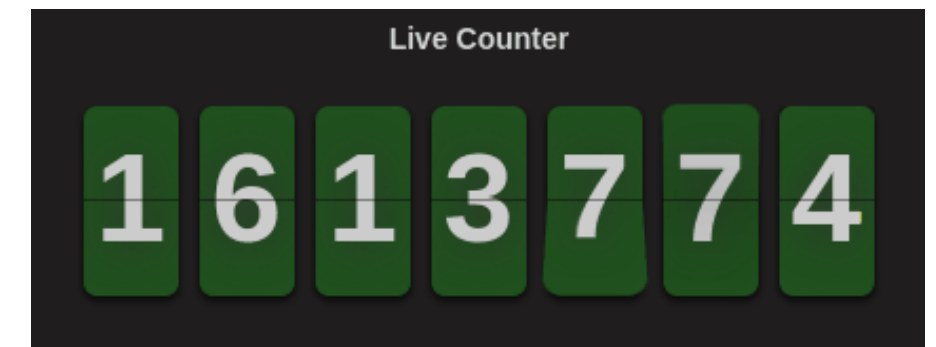
SCOPE OF THE PROBLEM



SCOPE OF THE PROBLEM



- One million seconds is roughly equal to 11.5 days.
- One billion seconds is roughly equal to 31.75 years.
- In 2017, there were 8.4 billion IoT devices.
- By 2020, that number exceeded 20.4 billion devices.
- Every second, another 127 devices are connected to the internet



SCOPE OF THE PROBLEM



Couple 'felt so violated' after hacker took over smart home devices, began talking to them

POSTED 5:31 PM, SEPTEMBER 23, 2019, BY TRIBUNE MEDIA WIRE

FACEBOOK REDDIT TWITTER PINTEREST LINKEDIN

Milwaukee couple warns hackers are outsmarting smart homes

FOX 6 NEWS

MILWAUKEE – A Milwaukee couple says their smart home was hacked after their camera began talking to them, and their thermostat reached upwards of 90 degrees.

Chicago Tribune

SECTIONS SEARCH

Why are you looking at me? I see you watching me.' Smart devices like Nest getting hacked in digital home invasions.

By ALLY MAROTTI
CHICAGO TRIBUNE | FEB 08, 2019 | 5:00 AM

Arjun Sud puts his 7-month-old son Oliver down for a nap in Lake Barrington. On Jan. 20, Sud heard a man's voice coming from the Nest camera mounted about his son's crib. The next cameras and thermostat in the Sud family's home had been hacked. (Erin Hooley/Chicago Tribune)

LATEST BUSINESS

Chicago cupcake-maker taking food truck fight to the U.S. Supreme Court

CPS teachers want an affordable

WHAT IS CYBERSECURITY?



CY-BER-SE-CUR-I-TY (NOUN) /,sībərsi'kyoʊrədē/

MEASURES TAKEN TO PROTECT A COMPUTER OR COMPUTER SYSTEM (AS ON THE INTERNET) AGAINST UNAUTHORIZED ACCESS OR ATTACK


SIMPLY PUT, CYBERSECURITY IS PROTECTION AGAINST DIGITAL ATTACKS.

THE DEPARTMENT OF HOMELAND SECURITY SAYS IT BEST:
“OUR DAILY LIFE, ECONOMIC VITALITY, AND NATIONAL SECURITY DEPEND ON A STABLE, SAFE, AND RESILIENT CYBERSPACE.”



THE REGIONAL IMPACT OF CYBER INCIDENTS






gt government technology

SECURITY

Some Offices Still Responding to Ransomware Attack

Nearly three-quarters of Louisiana state government workers continue to respond to the attack weeks ago.

BY SAM KARLIN, THE ADVOCATE / I



A vibrant night scene of a street in New Orleans, showing colorful buildings, balconies with lights, and a streetcar in the distance.

Ryuk ransomware implicated in City of New Orleans shutdown

Adam Bannister 18 December 2019 at 12:57 UTC
Updated: 06 January 2020 at 11:26 UTC

Cyber-attacks Ransomware Government

The malware has struck several US municipalities in 2019

ANALYSIS The cyber-attack that prompted the City of New Orleans' mayor to declare a state of emergency on Friday (December 13) is the latest in a string of attacks on city and state governments to be linked to the Ryuk ransomware.

% of Louisiana's State Government

,000 computer network servers that power operations across state government were damaged

m.



A photograph showing several people seated around a table in what appears to be a formal meeting or press conference.



Two large, empty rectangular boxes, likely placeholders for images or additional content.

THE LOCAL IMPACT OF CYBER INCIDENTS



Jasper County Incident – Oct 2019

Headline: “County computers attacked by ransomware in Jasper County”

Jasper County is trying to get back on track after hackers were able to get into the county’s computer systems. County officials say the problem started about three weeks ago.

Details on the origin of the ransomware and who put it into the system are still being investigated. Since it was found, the county has spent thousands of dollars trying to combat the issue, according to County Council Chairman Tom Johnson.

The systems are reportedly back up and running at this point, but Jasper County Sheriff Chris Malphrus is asking people to be patient when paying county taxes or bills until everything returns to normal. The sheriff also said his office will be working hard to catch up on entering data back into the system from the last few weeks.

CYBER CRIME BY THE NUMBERS



Let's put it in perspective:

- Tesla, Facebook, Microsoft, Apple, Amazon, and Walmart combined annual revenue totals "just" \$1.28 trillion.
- Cyber crime earns \$1.5 trillion annually.
- The \$1.5 trillion that cybercriminals earn is equal to Russia's gross domestic product (GDP)
- If cybercrime were a country, it would have the 13th highest GDP in the world.



CYBER CRIME BY THE NUMBERS



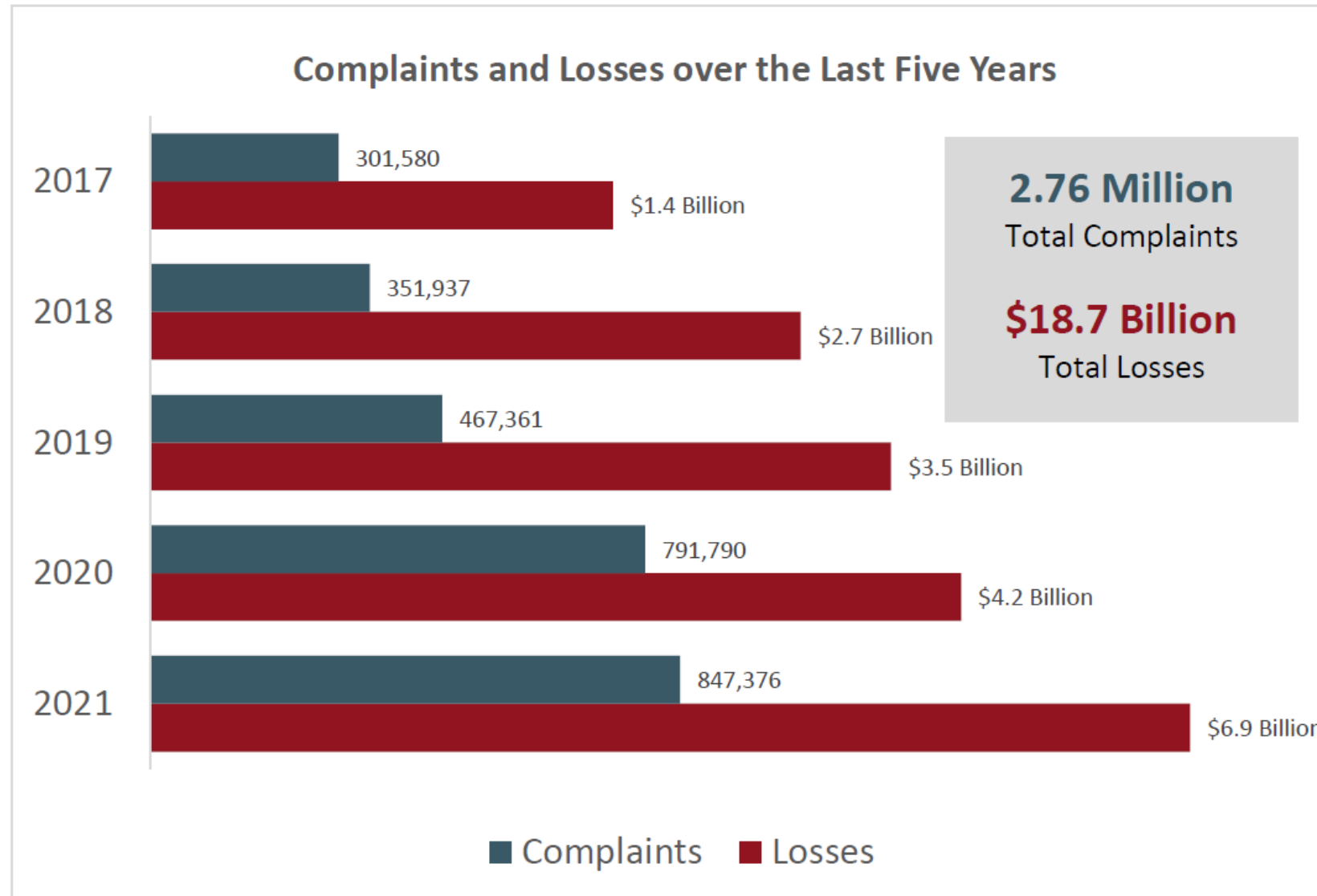
Let's put it in perspective:

- It's estimated that cybercrime will cost the world \$10.5 trillion annually by 2025.
- Organized criminal gangs account for 55% of attacks
- According to the FBI's IC3's 2021 Internet Crimes Report, there were 847,376 complaints of suspected internet crimes in the US, an increase of 7% from 2020.
- Those reported losses exceeded \$6.9 billion, an increase of 41% from 2020.



INTERNET CRIMES COMPLAINT CENTER

(IC3.GOV)



WHAT CAN YOU DO?



1. Notify Local Law Enforcement to report cyber crime.
2. Report cyber crime to IC3 via their website (ic3.gov).
3. For awareness purposes, please consider notifying SC Association of Counties of cyber incidents.
4. Ensure that your organization receives cybersecurity/phishing training.
5. Insist on multi-factor authentication for external access (email, OneDrive, VPN) to business apps and for important, personal apps for yourself (email, banking).
6. Ensure that your computer systems are secure and up to date.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY PROGRAM (SC CIC)

WHAT WE DO



1. PROVIDE NO-COST SECURITY SERVICES TO SOUTH CAROLINA'S CRITICAL INFRASTRUCTURE SECTORS
2. MAINTAIN THE CYBER LIAISON OFFICER, OR CLO, PROGRAM
3. LEAD THE SC CIC TASKFORCE, WHICH IS COMPRISED OF OUR FEDERAL AND STATE PARTNERS
4. OUR GOAL IS TO IMPROVE THE CYBER POSTURE OF SOUTH CAROLINA.

SC CIC MILESTONES



SC CIC Task Force



SC Law Enforcement Division
Oversees the SC CIC Program

SC Department of Administration
Division of Information Security



SC National Guard
125th Cyber Protection Battalion

US Department of Homeland Security
Cybersecurity & Infrastructure Agency



US Secret Service
Cyber Fraud Task Force

US Department of Homeland Security
Office of Intelligence and Analysis



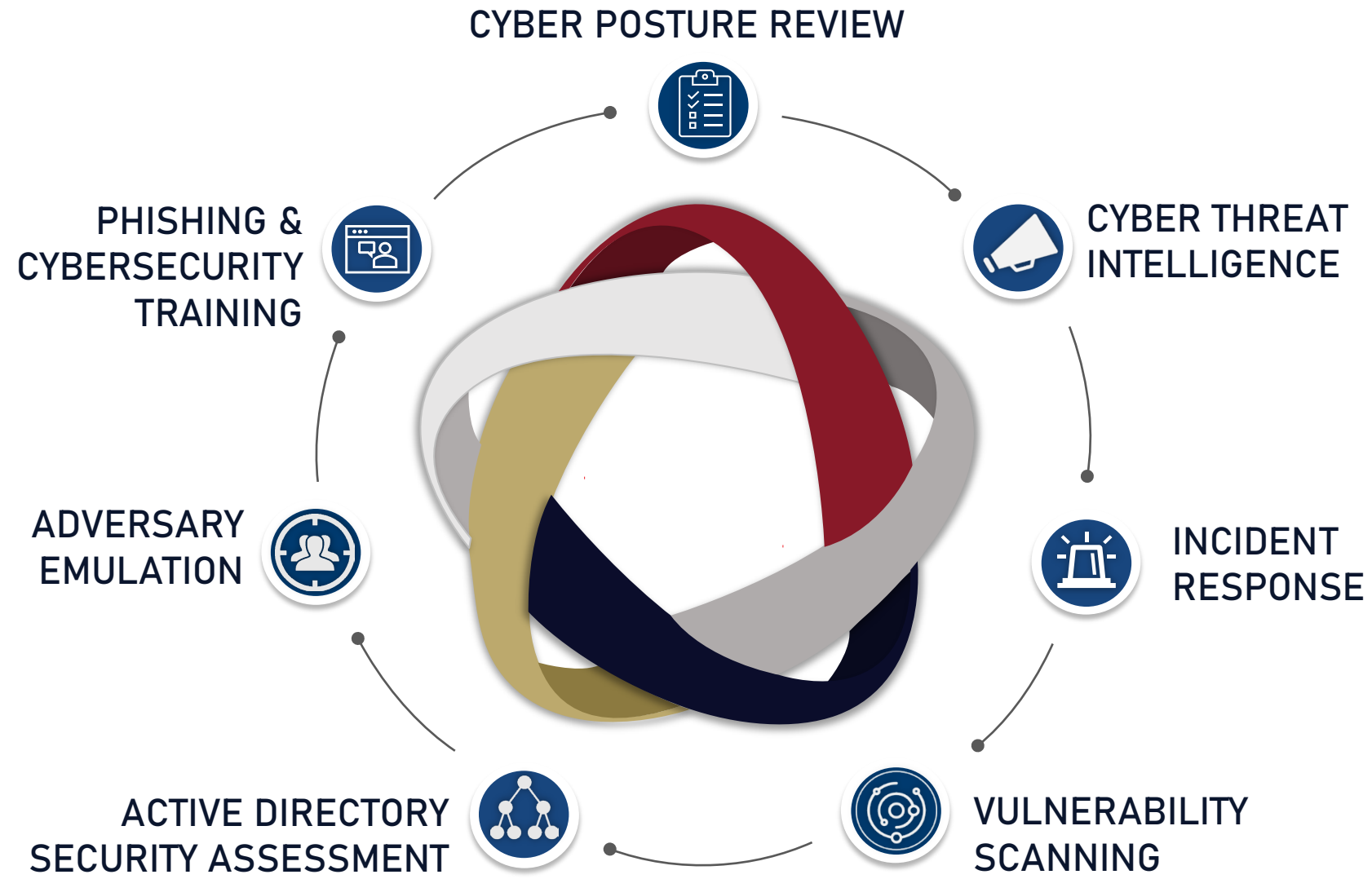
SC Emergency Management Division
Cyber Incident Consequence Management

Federal Bureau of Investigations
Cyber Squad

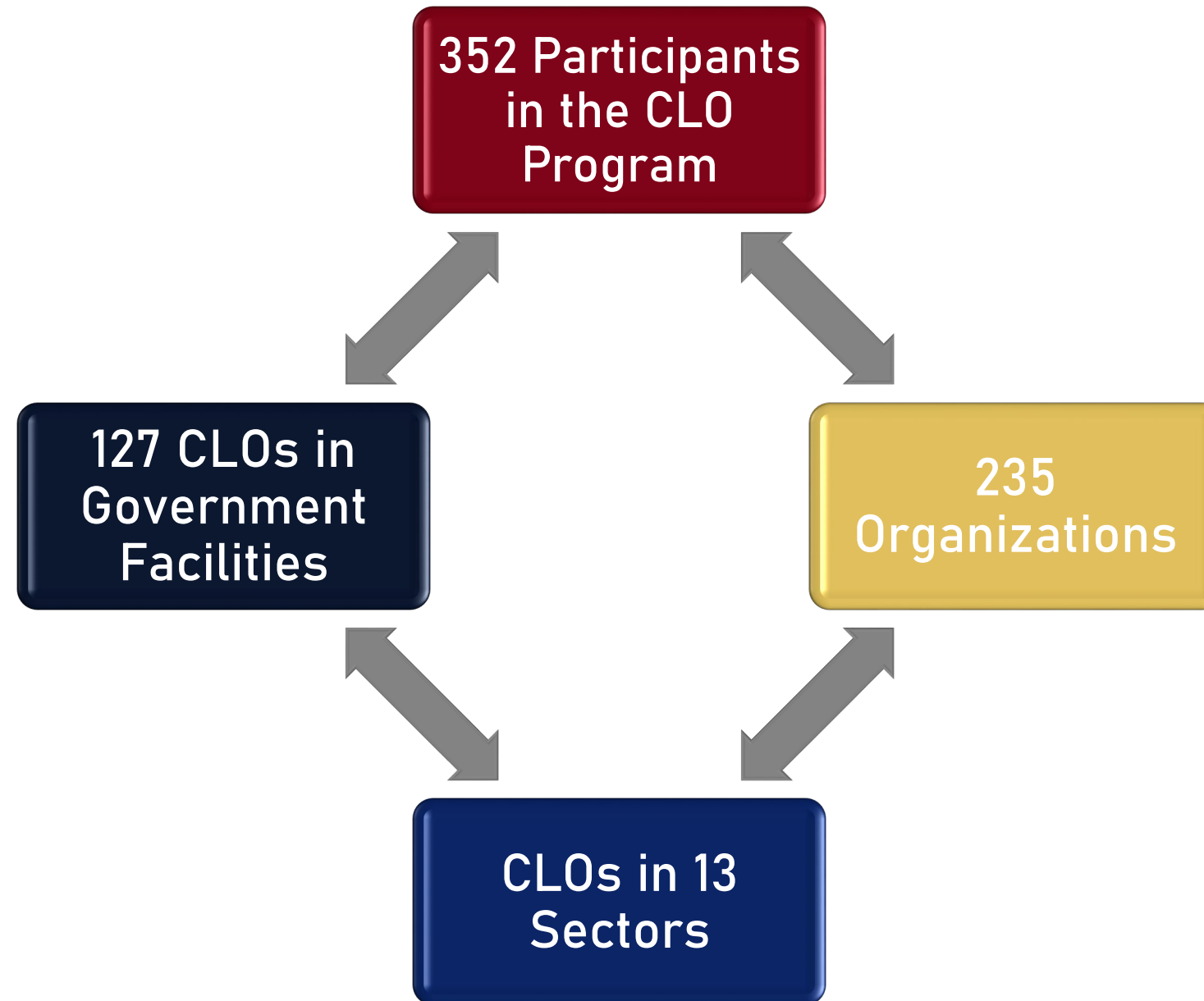


SC Election Commission
Election and Voter Information Security

SC CIC SERVICES



THE SC CIC CLO PROGRAM



THE SC CIC CLO PROGRAM



Intelligence
Sharing

Tabletop
Exercises

Networking
Opportunities

THE SC CIC TEAM



The SC CIC program is a national leader in redefining how cybersecurity services can be provided, intelligence distributed, and incident response performed at the state level.





Have any problems, questions, or concerns?

Please don't hesitate to reach out to the SC CIC team at

cyber@sled.sc.gov