



# Locking Down the Road: Navigating the Intersection of Cybersecurity and Trucking

Ryan Truskey | SLED CISO/CIO & Director of SC CIC

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

1



# SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY PROGRAM (SC CIC)

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

2

# WHAT WE DO

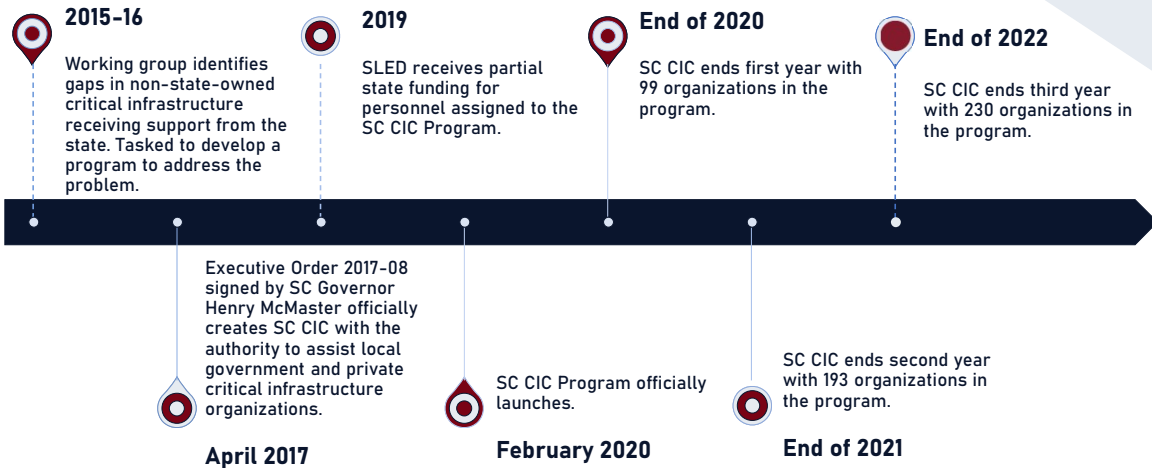


1. PROVIDE SECURITY SERVICES TO SOUTH CAROLINA'S CRITICAL INFRASTRUCTURE SECTORS
2. FACILITATE THE CYBER LIAISON OFFICER (CLO) PROGRAM
3. LEAD THE SC CIC TASK FORCE, COMPRISED OF FEDERAL AND STATE PARTNERS
4. IMPROVE THE CYBER POSTURE OF SOUTH CAROLINA.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

3

# SC CIC MILESTONES

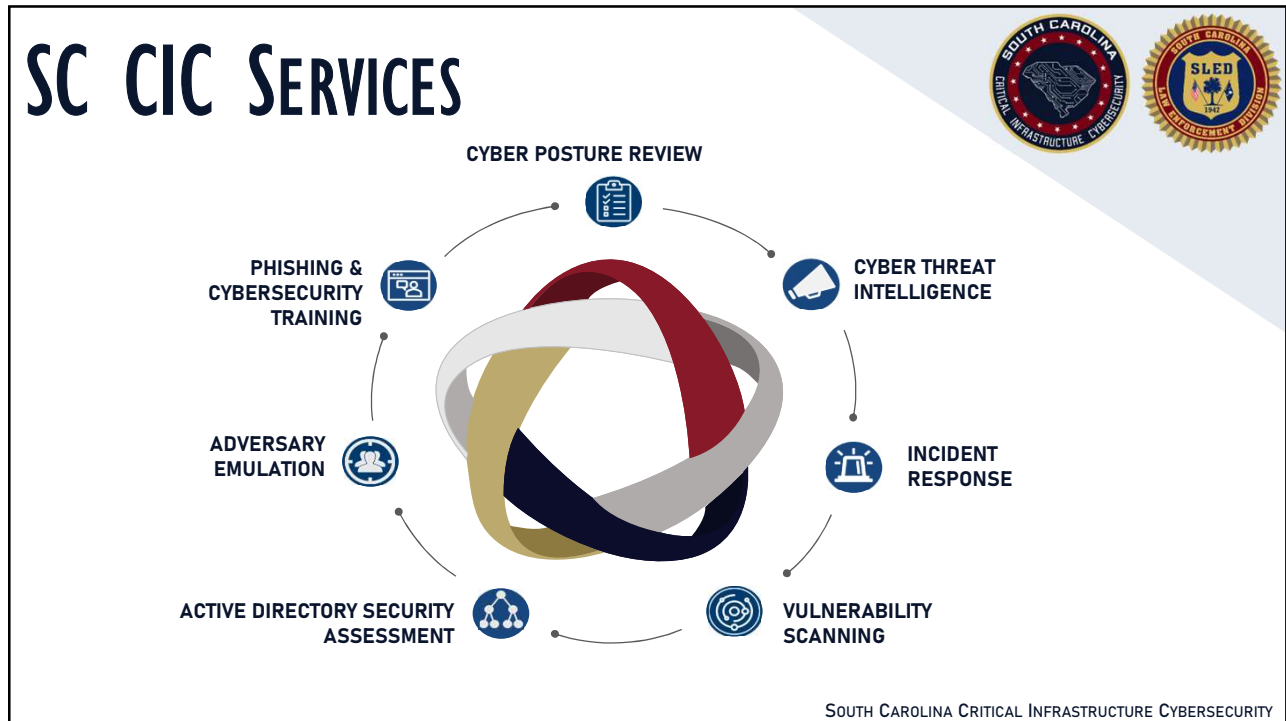


SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

4





5



6

# THE SC CIC CLO PROGRAM



247 Organizations

13 out of the 16 Critical Infrastructure Sectors

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

7

# THE SC CIC CLO PROGRAM



Intelligence Sharing

Tabletop Exercises

Networking Opportunities

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

8

# THE SC CIC TEAM



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



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

# CYBERSECURITY IN THE TRANSPORTATION SECTOR



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

# CRITICAL INFRASTRUCTURE SECTORS



Chemical	Dams	Financial Services	Information Technology
Commercial Facilities	Defense Industrial Base	Food & Agriculture	Nuclear Reactors, Materials, & Waste
Communications	Emergency Services	Government Facilities	Transportation Systems
Critical Manufacturing	Energy	Healthcare & Public Health	Water & Wastewater

[HTTPS://WWW.CISA.GOV/CRITICAL-INFRASTRUCTURE-SECTORS](https://www.cisa.gov/critical-infrastructure-sectors)

11

# CYBER THREAT ACTORS



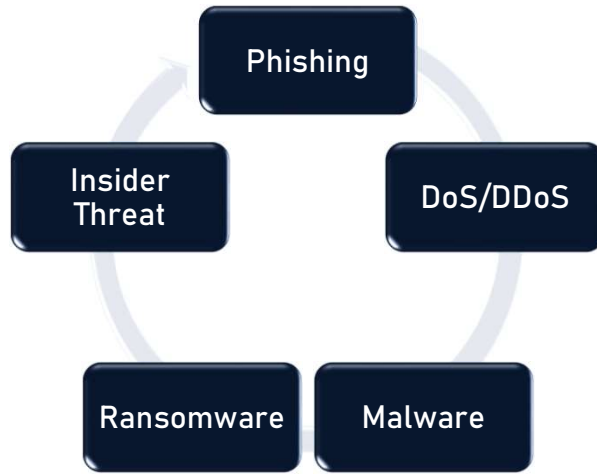
## Common Threat Actors & Motivations



<https://www.sentinelone.com/cybersecurity-101/threat-actor/>

12

# THE ANATOMY OF CYBER THREATS

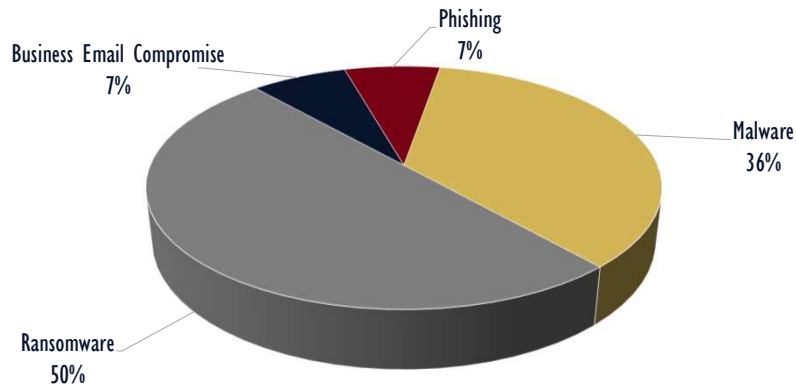


13

# CYBER INCIDENTS IN SOUTH CAROLINA



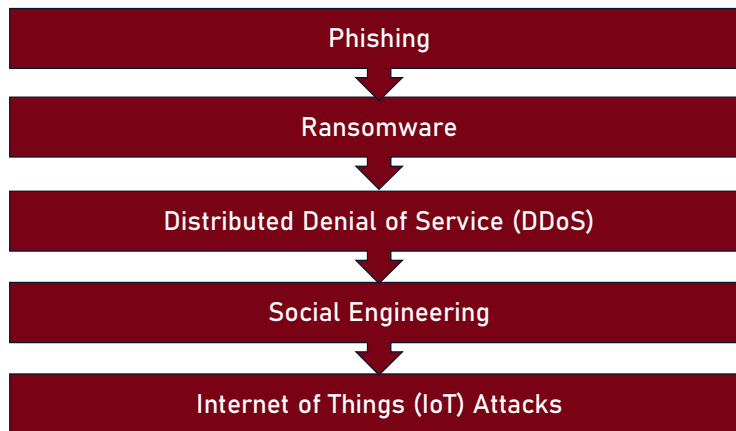
Types of Incidents in SC in 2022



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

14

# COMMON THREATS TO THE TRANSPORTATION SECTOR



[HTTPS://NMFTA.ORG/TOP-10-CYBER-THREATS-FACING-THE-TRUCKING-INDUSTRY-TODAY-AND-WHAT-TO-DO-ABOUT-THEM/](https://nmfta.org/top-10-cyber-threats-facing-the-trucking-industry-today-and-what-to-do-about-them/)

15

# MAERSK NOTPETYA ATTACK 2017



- THREAT ACTORS GAINED ACCESS THROUGH THE SOFTWARE, M.E. DOC, WHICH WAS INSTALLED ON A SINGLE WORKSTATION IN A UKRAINIAN PORT CITY.
- THE IMPACT OF NOTPETYA AT MAERSK INCLUDED:
  - 50,000 INFECTED ENDPOINTS
  - 1000S OF APPLICATIONS & SERVERS
  - 600 SITES IN 130 COUNTRIES
- IT TOOK MAERSK 10 DAYS TO REBUILD THE INFRASTRUCTURE
- \$300 MILLION DOLLARS IN LOSSES



[HTTPS://WWW.WIRED.COM/STORY/NOTPETYA-CYBERATTACK-UKRAINE-RUSSIA-CODE-CRASHED-THE-WORLD/](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/)  
[HTTPS://WWW.ZDNET.COM/ARTICLE/RANSOMWARE-THE-KEY-LESSON-MAERSK-LEARNED-FROM-BATTLING-THE-NOTPETYA-ATTACK/](https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/)

16



# FORWARD AIR ATTACK 2020



- IN DECEMBER 2020, FORWARD AIR WAS VICTIM TO A RANSOMWARE ATTACK.
- \$7.5 MILLION LOST IN LTL FREIGHT REVENUE
- PERSONAL INFORMATION OF FORWARD AIR EMPLOYEES WAS EXFILTRATED AND LEAKED BY THREAT ACTORS



[HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/TRUCKING-GIANT-FORWARD-AIR-REPORTS-RANSOMWARE-DATA-BREACH/](https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-reports-ransomware-data-breach/)  
[HTTPS://WWW.BLEEPINGCOMPUTER.COM/NEWS/SECURITY/TRUCKING-GIANT-FORWARD-AIR-HIT-BY-NEW-HADES-RANSOMWARE-GANG/](https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-hit-by-new-hades-ransomware-gang/)

17

# BAY & BAY RANSOMWARE INCIDENT 2021



- THE CONTI RANSOMWARE GROUP GAINED ACCESS THROUGH A KNOWN MICROSOFT EXCHANGE SERVER VULNERABILITY THAT HAD NOT BEEN UPDATED YET.
- THE RANSOMWARE ATTACK IMPACTED SOME OF THE CARRIER'S SYSTEM AND A SMALL PORTION OF DESKTOP COMPUTERS.
- THE CARRIER WAS ABLE TO 90% OPERATIONAL WITHIN A DAY AND A HALF



[HTTPS://WWW.FREIGHTWAVES.COM/NEWS/MINNESOTA-TRUCKING-COMPANY-HIT-IN-2ND-RANSOMWARE-ATTACK](https://www.freightwaves.com/news/minnesota-trucking-company-hit-in-2nd-ransomware-attack/)

18

# WHY SHOULD CYBERSECURITY MATTER?



1. MANY OF THE U.S.' CRITICAL INFRASTRUCTURE SECTORS RELY ON TRANSPORTATION FOR DAILY OPERATIONS.
2. A CYBER ATTACK COULD HAVE A DETRIMENTAL IMPACT ON AN ORGANIZATION'S DAILY OPERATIONS & OVERALL REPUTATION.
3. CYBER THREATS AGAINST CRITICAL INFRASTRUCTURE ARE CONSTANTLY EVOLVING AND GROWING IN COMPLEXITY.



[HTTPS://WWW.CISA.GOV/SITES/DEFAULT/FILES/PUBLICATIONS/NIPP-SSP-TRANSPORTATION-SYSTEMS-2015-508.PDF](https://www.cisa.gov/sites/default/files/publications/NIPP-SSP-TRANSPORTATION-SYSTEMS-2015-508.PDF)

19

# WHAT YOU CAN DO



1. UNDERSTAND THAT SECURITY IS A CONTINUOUS LIFE-CYCLE.
2. KNOW THAT GOOD SECURITY POSTURE WITHIN AN ORGANIZATION BEGINS WITH THE BASICS.
3. HELP PROMOTE A CULTURE OF CYBERSECURITY WITHIN YOUR ORGANIZATION.
4. UTILIZE AVAILABLE RESOURCES TO HELP STRENGTHEN YOUR ORGANIZATION.

<https://www.linkedin.com/pulse/what-ceos-boards-should-know-cybersecurity-ciso-role-gary-hayslip>  
<https://www.forbes.com/sites/forbestechcouncil/2018/01/05/the-ceos-critical-role-in-driving-cybersecurity-readiness/?sh=6f2cc17b4170>

20



Have any problems, questions, or concerns?

Want to join the SC CIC program?

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

**cyber@sled.sc.gov**

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY