WECC Cybersecurity Event Trends

Cyber Security Work Group

October 20, 2022

Lenin Maran, CSWG Chair

John Graminski, Staff Liaison

Cybersecurity Event Trends

- WECC Cybersecurity Event Reporting
  - Form DOE-417
  - WECC Reported Cybersecurity Events
- E-ISAC Cybersecurity Event Reporting
  - ERO-Wide Cybersecurity Events
- Other Cybersecurity Trends
  - Cybersecurity Challenges with DER Implementations

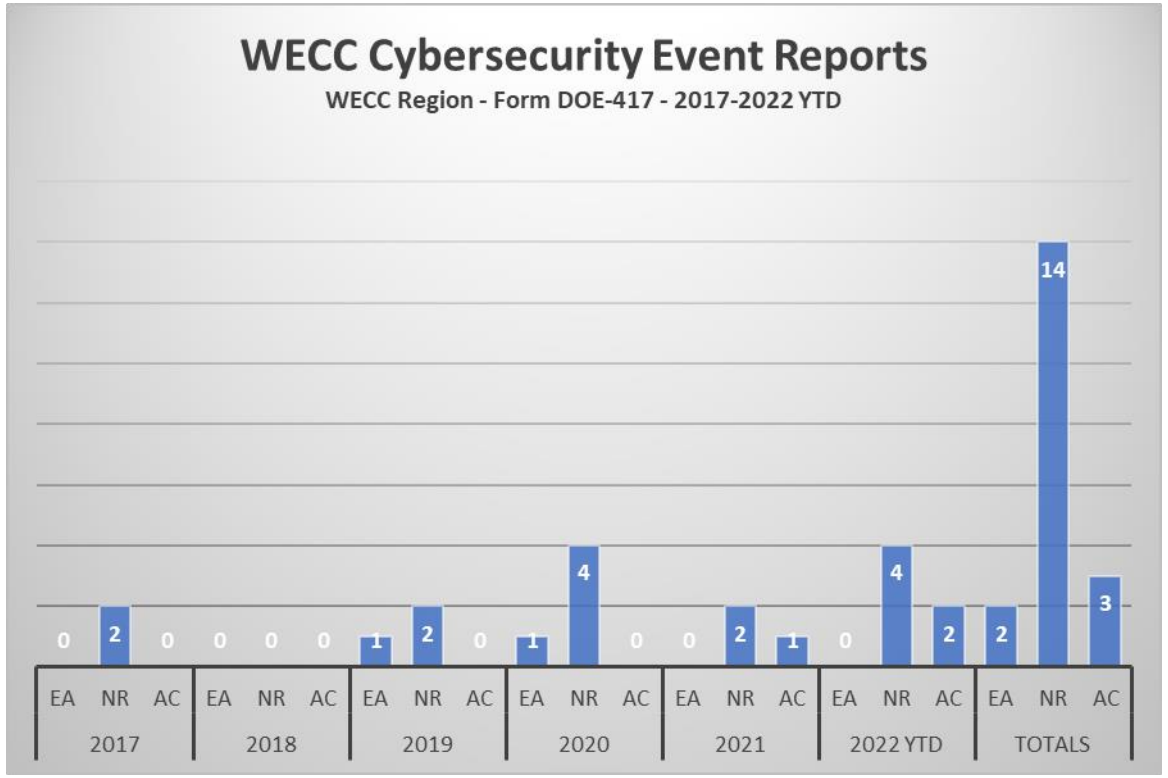
Form DOE-417 Cybersecurity Definitions

- **Cyber event**: A disruption on the electrical system or communication system(s) caused by unauthorized access to computer software and communications systems or networks including hardware, software, and data (DOE-417 Instructions, Page 8).
- **Cyber Security Incident**: A malicious act or suspicious event that:
  - For a high- or medium-impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
  - Disrupts or attempts to disrupt the operation of a BES Cyber System (NERC Glossary, Page 10).
- **Reportable Cyber Security Incident**: A Cyber Security Incident that compromised or disrupted:
  - A BES Cyber System that performs one or more reliability tasks of a functional entity;
  - An Electronic Security Perimeter of a high- or medium-impact BES Cyber System; or
  - An Electronic Access Control or Monitoring System of a high- or medium-impact BES Cyber System (NERC Glossary, Page 10).

Form DOE-417 Cybersecurity Reports

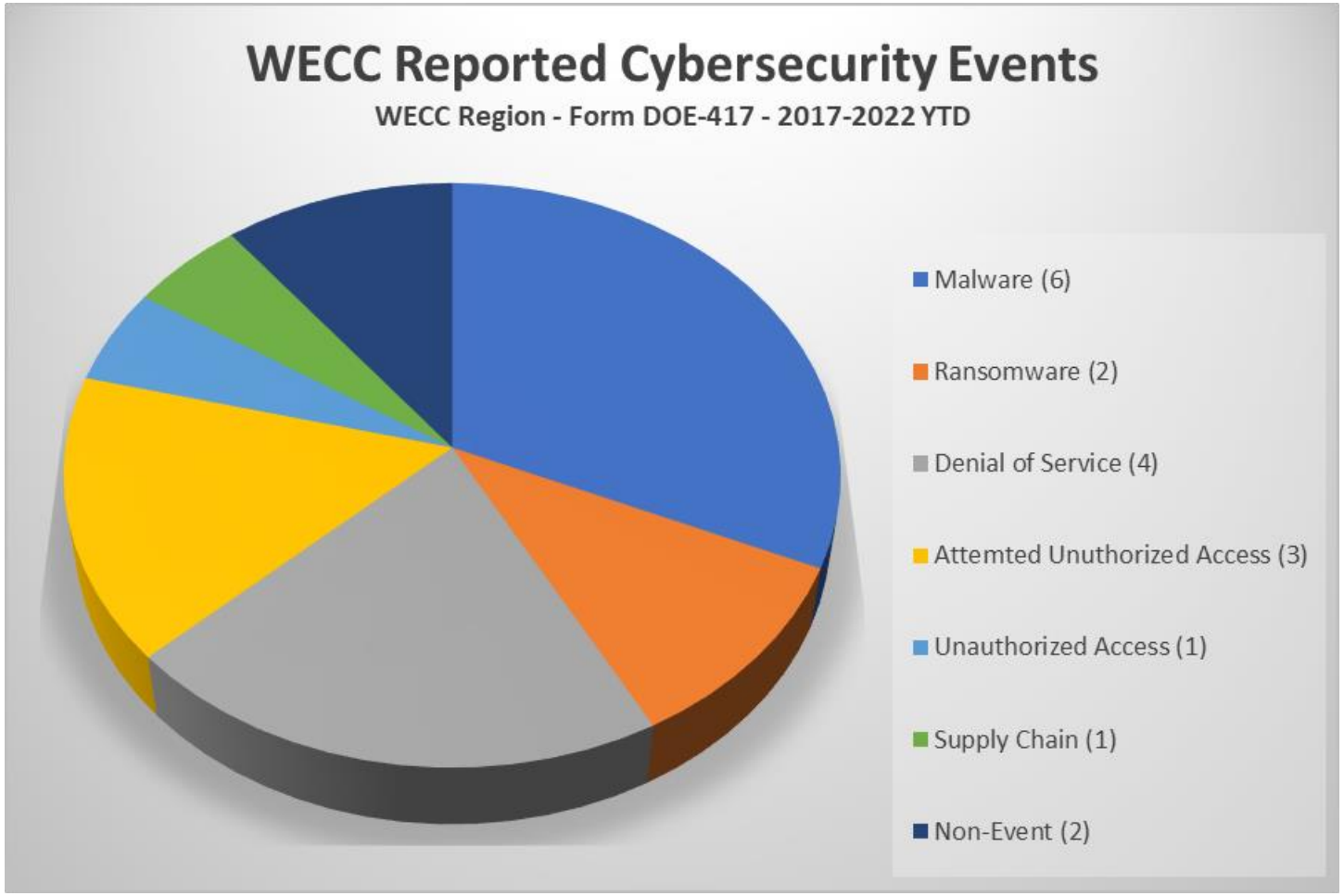
- **Emergency Alert**: Required within one hour of:
  - A *Reportable Cyber Security Incident*; or
  - A cyber event that is not a *Reportable Cyber Security Incident* that causes interruptions of electrical system operations.
- **Normal Report**: Required within six hours of a *cyber event* that could potentially affect electric power system adequacy or reliability.
- **Attempted Cyber Compromise**: Required within one day of a *Cyber Security Incident* that was an attempt to compromise a high- or medium-impact BES Cyber System or its associated Electronic Access Control or Monitoring Systems (EACMS).

WECC Cybersecurity Event Reports



EA: Emergency Alert - Causes interruptions of electrical system operations
NR: Normal Report - Potentially impacts electric power system adequacy or reliability
AC: Attempted Cyber Compromise – High- or medium-impact BCS or associated EACMS

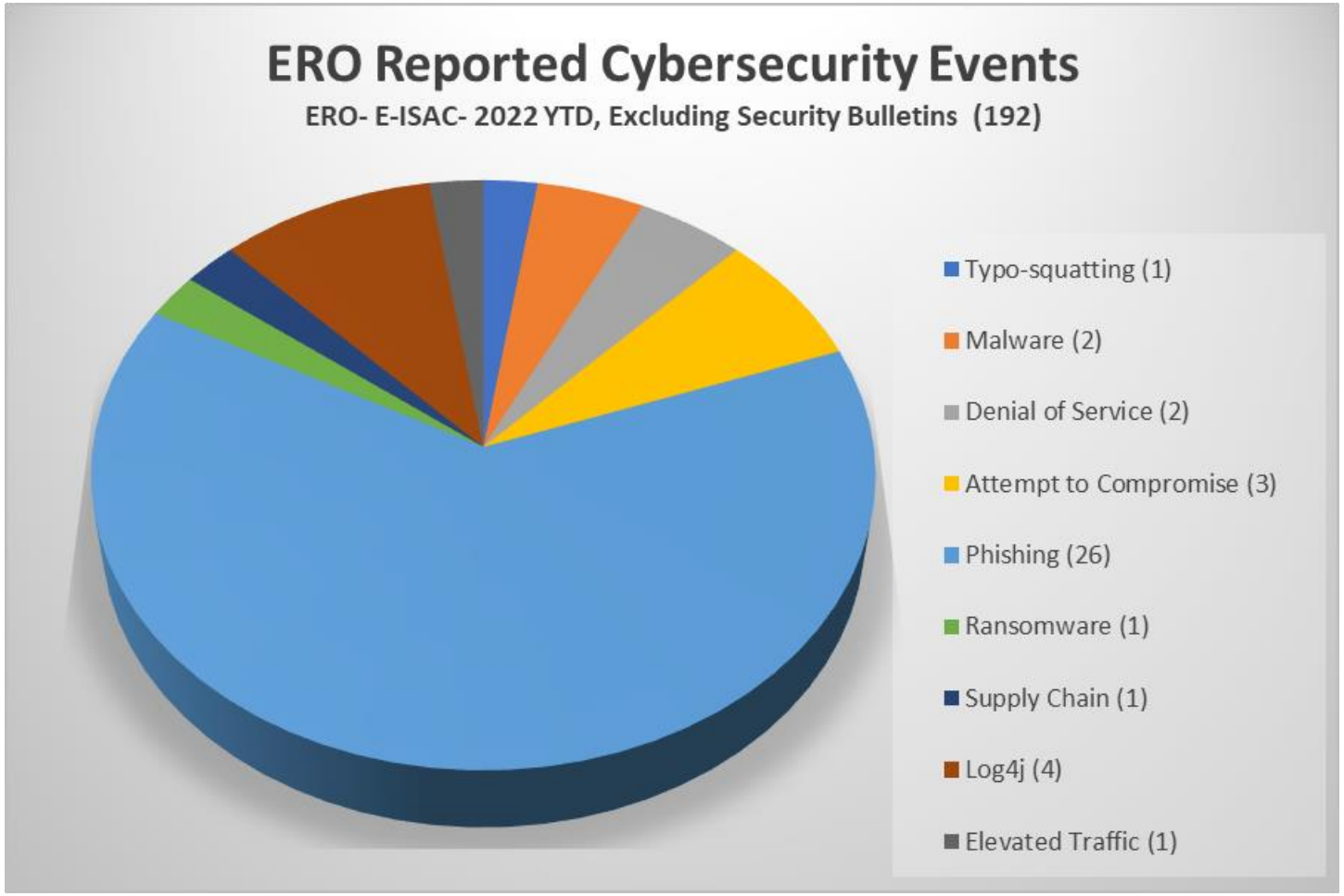
WECC Reported Cybersecurity Event Types



E-ISAC Cybersecurity Reports

- E-ISAC Authored Reports (Bulletins)
  - ICS Security Bulletin
  - Weekly Vulnerabilities Summary
  - Weekly Cybercrime Forum and Ransomware Report
  - Monthly Report
- ERO Entity-Supplied Cybersecurity Reports
  - Form DOE-417
  - Direct Reporting

ERO Reported Cybersecurity Event Types



Cybersecurity Challenges with DER Implementations

- Influx of devices and technology to support climate change and carbon reduction efforts in the next 5–10 years
- Utilities may not own or operate these devices
- No defined role, cyber compliance obligations yet for DER operators
- Insufficient assessment of DER vulnerability and attack on grid
- Supply chain security
- Lack of defined and auditable cybersecurity Standards
- Patch management
- Access management

WECC

Electric Reliability and Security for the West

Contact:

Lenin Maran
lenin.maran@smud.org
John Graminski
jgraminski@wecc.org

References

- *Form DOE-417, Electric Emergency Incident and Disturbance Report*, OMB No. 1901-0288. Available: https://www.oe.netl.doe.gov/docs/OE417_Form_05312024.pdf.
- *Form DOE-417 Instructions*, OMB No. 1901-0288. Available: https://www.oe.netl.doe.gov/Docs/OE417_Form_Instructions_05312024.pdf.
- *Glossary of Terms Used in NERC Reliability Standards*, March 29, 2022. Available: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.
- *Electricity Information Sharing and Analysis Center (E-ISAC) Portal*. Available: https://www.eisac.com.