NETWORK RESILIENCY

GULF COAST ELECTRIC COOPERATIVE

April 13, 2022

Justin Barnes

VP of Member Services

CYBERSECURITY FACTS

- **A cyber attack happens every 39 seconds**
  - Study found that computers are hacked 2,244 times a day on average
- **Average lifecycle of a breach is 279 days**
  - Basically 9 months before an identified breach can be controlled
- **94% of all malware attacks are carried out through email**
- **Human error is the primary cause for cybersecurity breaches, 95%**
  - Weak Passwords and downloading malicious attachments

GCEC Incident

- July 23, 2021 – Phishing email received and opened at GCEC (no knowledge at this time)
- August 14, 2021 – Attack was initiated on GCEC's Information System
  - All but one server was locked down with encrypted files. Ransom note was left on the server
- August 14-15, 2021 – Rebuilt servers and reimaged all "affected" workstations
  - Affected workstations had local admin users set up along with encrypted and .NYSQL files
- August 15, 2021 – Meridian (CIS & FIS) along with Milsoft OMS were both restored
  - **Tropical Storm Fred scheduled to make direct landfall in our area 8/16/22**
- August 17, 2021 – Initiated a second attack on our system
- August 18, 2021 - FBI was contacted and we proceeded with direction given
  - Completely rebuild Active Directory with new domain
  - Reimage ALL servers and workstations that were connected to the network at time of attack
  - Installed Carbon Black Antivirus Endpoint Protection on all devices and servers

Cyber Incident Effect on Daily Operations

- Meridian Operating System (CIS & FIS) Down
- Milsoft Outage Management System Down
- Futura Mapping Down
- TWACS AMI Metering System Down
- Partner Staking Down

GCEC Incident

- August 25, 2021 – Futura Mapping was restored
  - 11 Days
- August 27, 2021 – AMI system (TWACS) was restored
  - 13 Days
- January 13, 2022 – Partner Staking was restored
  - 139 Days

Cybersecurity Network Defense

- **EMPLOYEE EDUCATION**
- Strong Firewall Configurations
- Modern Antivirus Software with Endpoint Detection
- Multi-Factor Authentication
- Strong Data Backup System

How Does This Tie To Hurricanes???

- **October 10, 2018 Hurricane Michael made a direct landfall in GCEC's service territory.**
  - None of GCEC's 21,000+ meters had power
  - Workforce grew from 75 employees to over 1,600
  - Replaced over 3,500 poles
  - Replaced over 2,100 transformers
  - Replaced over 350 miles of line

  - Total debt incurred due to storm closing in on $100 million

  - Interest Expense on Line of Credit was approximately $268,000 per month.

How Does This Tie To Hurricanes???

- Operational Setbacks due to Hurricane Michael
  - **Hardware Protection**
    - Ensure servers and equipment are in a safe place
  - **No Communication**
    - No Internet, Phones or Cell Phones
  - **No CIS or FIS Operating System**
    - No billing, payments, payroll or AP payments could be processed
  - **No Milsoft Outage Management System**
    - No way for members to report outage or for us to have a quick reference for numbers
  - **No Futura Mapping**
    - No access to electronic maps for GCEC Employee or Contract Crews to utilize
  - **No Partner Staking**
    - No way to draw up jobs that required staking sheets electronically

No Communications

- **Internet and Phones Down for Weeks Post Hurricane**
  - Most aerial phone and communication lines were taken down during the storm. Post storm, there was a constant battle with debris trucks ripping down lines that were hanging low
  - Acquired two alternative fiber feeds into each of our offices as well as a pep-link cellular router for network backup. Ability to feed internet via microwave from our G&T radio towers.
  - Moved away from our on-site Voice/IP phone system and went to a cloud-based provider with multiple operation centers for redundancy.

- **Cell Phone communications were down across our territory**
  - Verizon is our primary provider based off coverage capability
  - Purchased First-Net AT&T cell phones for backup use in emergency situations.

No CIS or FIS Operating Systems

- Acquired two alternative fiber feeds into each of our offices as well as a Verizon cellular router for network backup. Ability to feed internet via microwave from our G&T radio towers

- Have dedicated communication links set up between each of our three offices with cellular failover and alternate VPN tunnels built in the event the dedicated circuits go down.

No Milsoft Outage Management System

- Had territory maps printed out based off grids and were able to distribute those maps to contractors and GCEC employees to be able to accurately restore power to GCEC members

- Installing smart boards in each of our offices that will assist in the restoration process

No Futura or Partner Mapping/Staking

- With Partner Staking down, we were unable to draw any jobs electronically or produce any picking tickets for materials to be pulled from the warehouse.
  - Stakers went out into the field with specified job areas surveying damages and drawing up material that would be needed to restore those particular damaged areas.
  - The list would be turned into the Warehouse crew that would then pull the materials and bundle it all on pallets with specific job numbers that would be given to the crew leader each morning with paper maps of the location specific to their material.

Any Questions or Comments?