

Colonial Pipeline Cyber Attack

Presented by Adalberto Trujillo

Table of Contents

I

Overview of the Emergency

- › Description of Emergency
- › Why is it an Emergency?

II

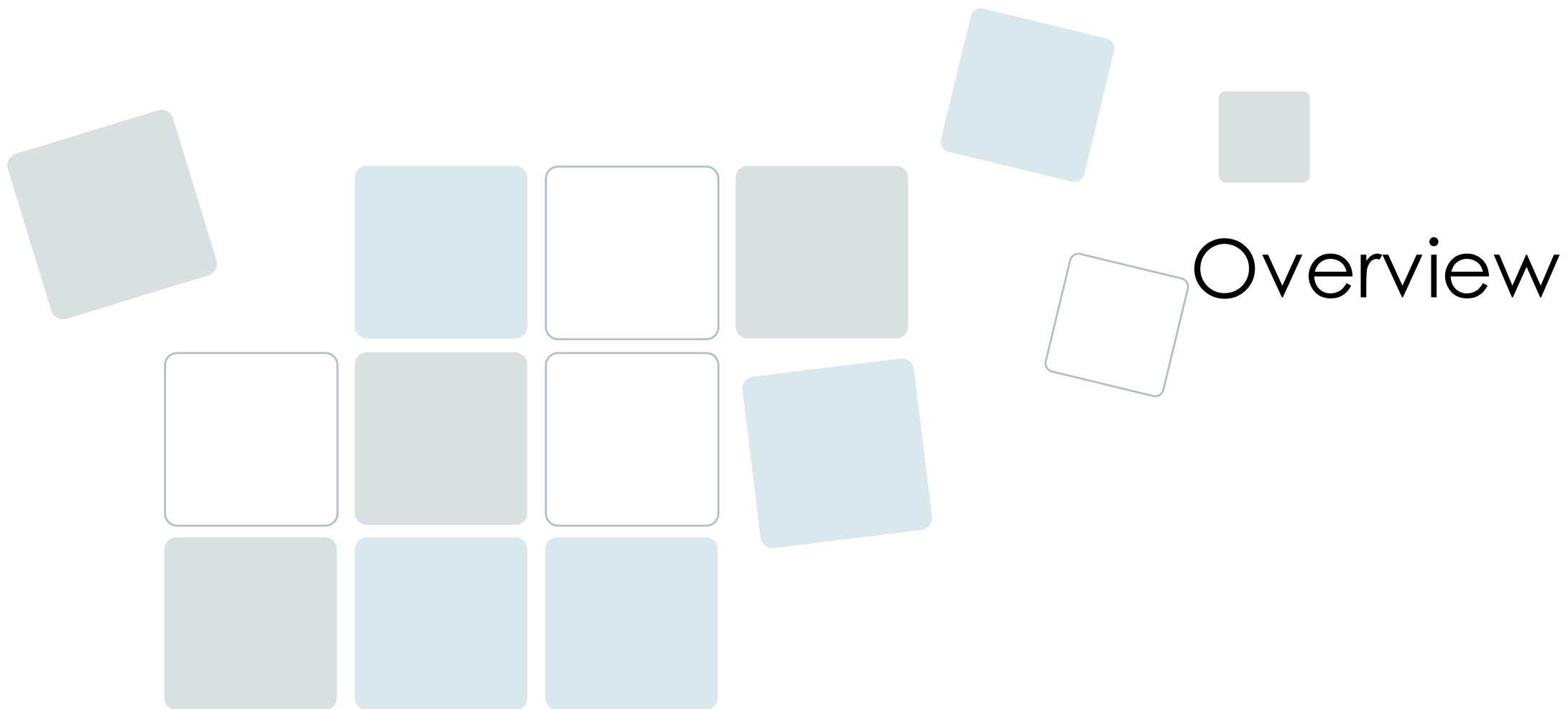
Crisis Management Cycle Overview

- › Response
- › Recovery
- › Prevention
- › Preparedness

III

Lessons Learned

- › Lessons Learned and Q&A



100 MILLION GALLONS OF FUEL TRANSPORTED PER DAY

Fuel
provided for



of the East Coast
of the United States

Fueling the
East Coast since

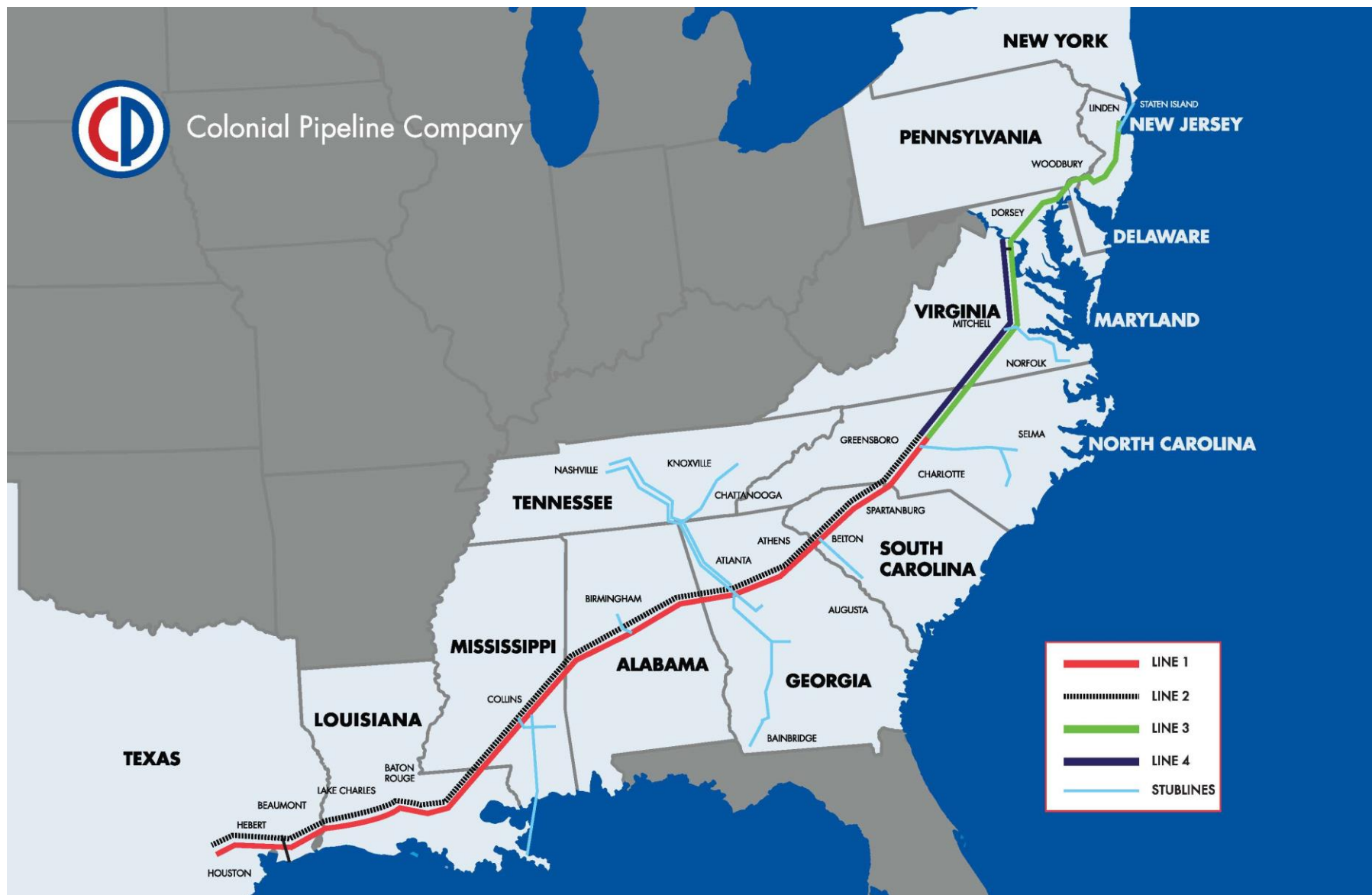


Transports fuel
for more than





Colonial Pipeline Company



Colonial Pipeline Hit By Ransomware Cyber Attack

TIMELINE OF EVENTS

FRIDAY, MAY 7



- Colonial Pipeline becomes aware of a ransomware attack subsequently attributed to the Darkside group
- Digital systems are taken offline to contain the threat
- Colonial engages leading third-party cybersecurity firm and activates incident response team
- The FBI, CISA, FERC, PHMSA, U.S. Department of Energy and Homeland Security are notified of the incident
- Colonial releases the first of eight statements informing the public about the ransomware attack

SATURDAY, MAY 8 – SUNDAY, MAY 9



- Colonial begins daily coordination meetings with the federal government led by Department of Energy
- Colonial begins daily on-the-ground and aerial system integrity monitoring across 5,500 mile pipeline footprint
- Colonial begins to manually operate some smaller lateral lines between terminals and delivery points while existing inventory is available
- Colonial's operational team begins development of a system restart plan

MONDAY, MAY 10 – TUESDAY, MAY 11



- The FBI confirms ransomware is responsible for the incident
- Colonial continues to work with the Department of Energy and customers to identify where product shortage may exist and prioritize those locations
- Federal and state governments take emergency actions to help alleviate disruptions to the fuel supply chain

WEDNESDAY, MAY 12



- Colonial restarts pipeline operations at approximately 5:00 p.m. ET



Federal Motor Carrier
Safety Administration

May 9, 2021

REGIONAL EMERGENCY DECLARATION
UNDER 49 CFR § 390.23
No. 2021-002

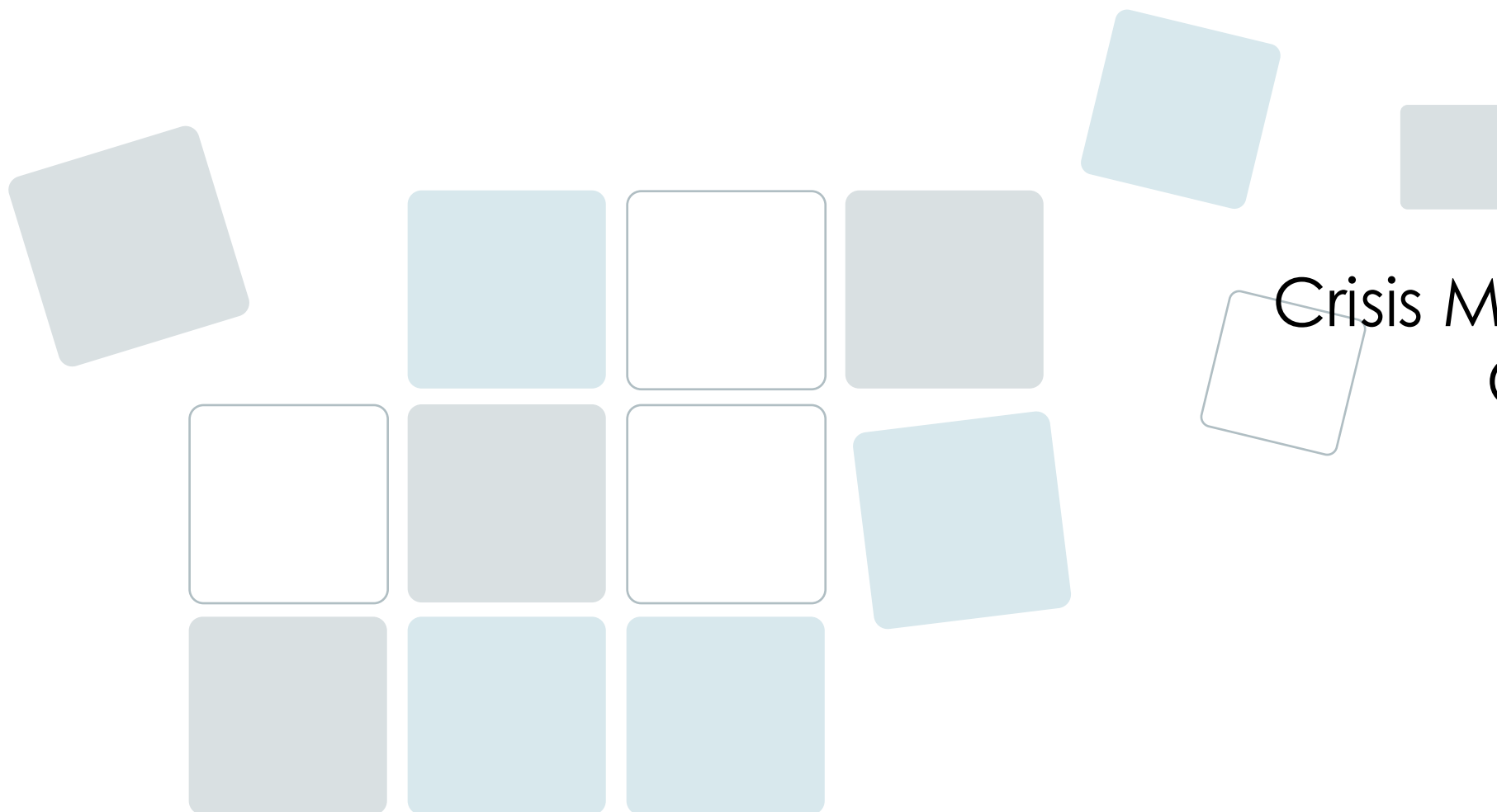
**ALABAMA, ARKANSAS, DISTRICT OF COLUMBIA, DELAWARE, FLORIDA,
GEORGIA, KENTUCKY, LOUISIANA, MARYLAND, MISSISSIPPI, NEW JERSEY,
NEW YORK, NORTH CAROLINA, PENNSYLVANIA, SOUTH CAROLINA,
TENNESSEE, TEXAS, AND VIRGINIA**

**State of
Emergency
Declared**

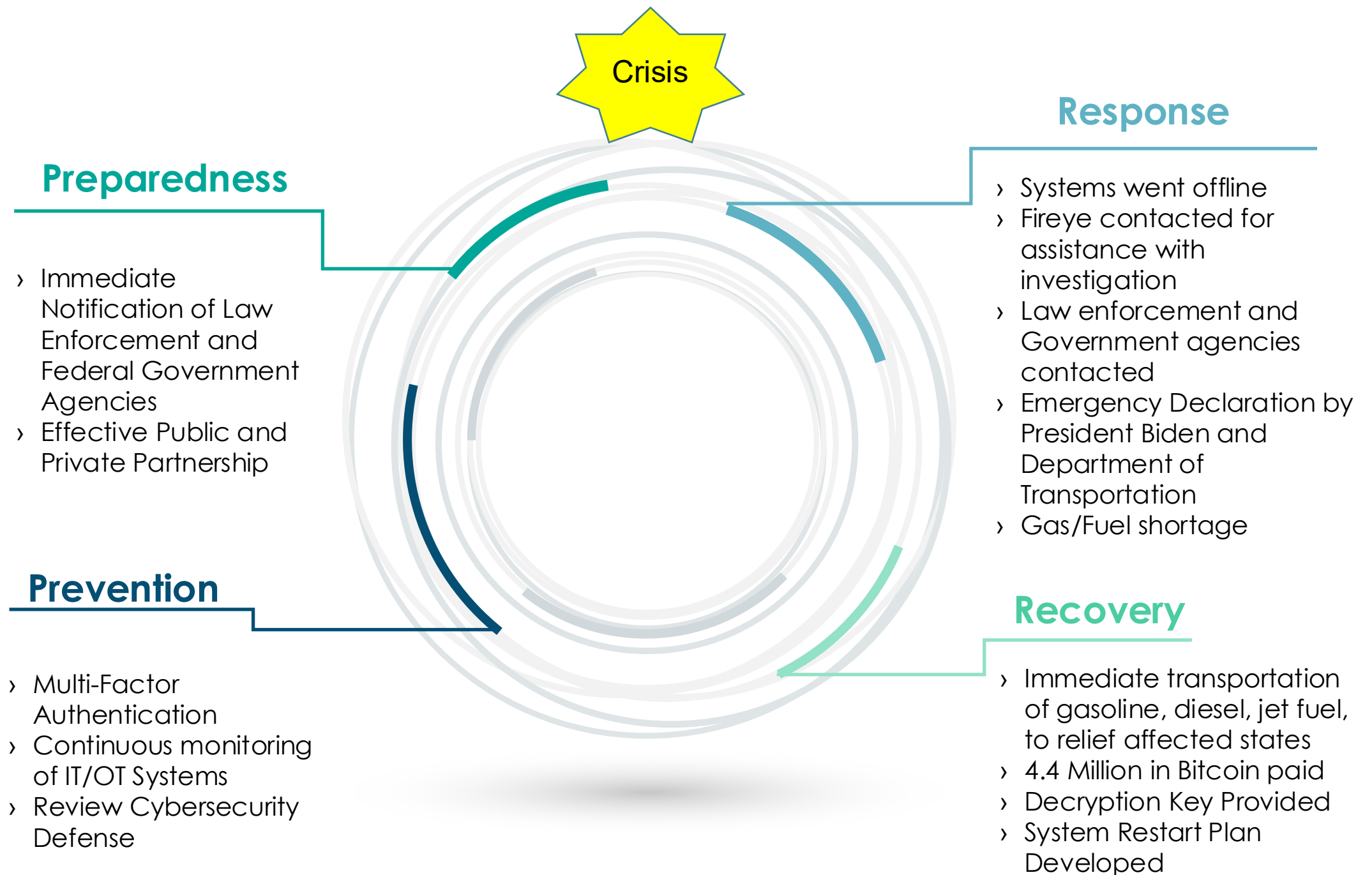


Public Response





Crisis Management Cycle





RANSOMWARE BEHIND THE SCENES

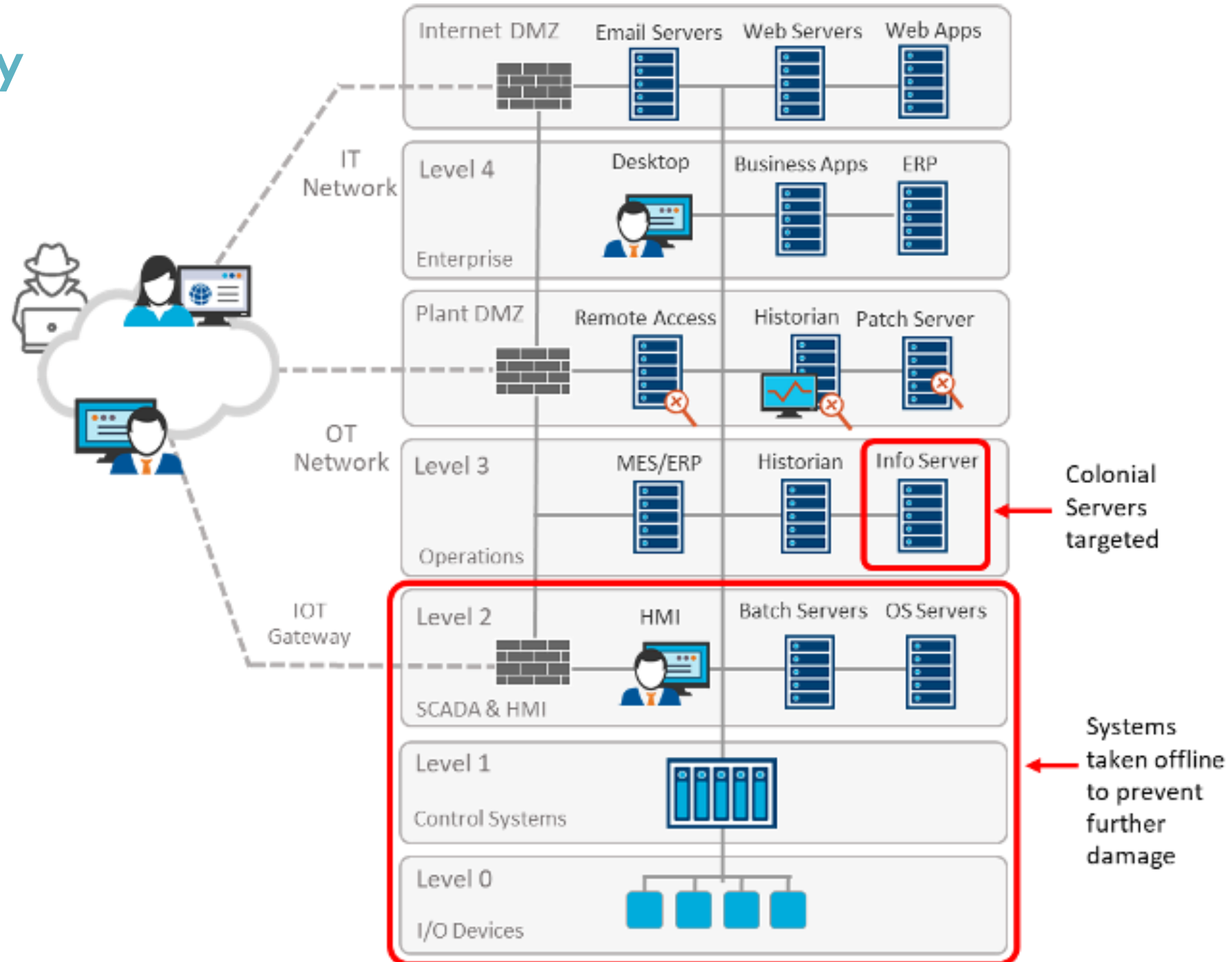
By the time victims see the ransom note, it's already too late—ransomware has already encrypted files before they know it's there. Here's what happens between infection and the ransom demand.



- A re-used password was discovered inside a batch of leaked passwords on the dark web which were all compromised in a data breach
- Compromised Password was used by a Colonial Pipeline Employee on a legacy VPN Profile to access their network remotely
- On May 7th, 2021, at 5:00 AM, Ransomware Payload Initiated and infected multiple computers and Colonial Pipeline's Network
- Darkside grabbed files totaling up to 100 GB stored on Colonial Pipeline's Shared-Drive
- Encrypted files and demanded nearly 5 million in crypto paid in Bitcoin, files were inaccessible to all Colonial Pipeline Employee's

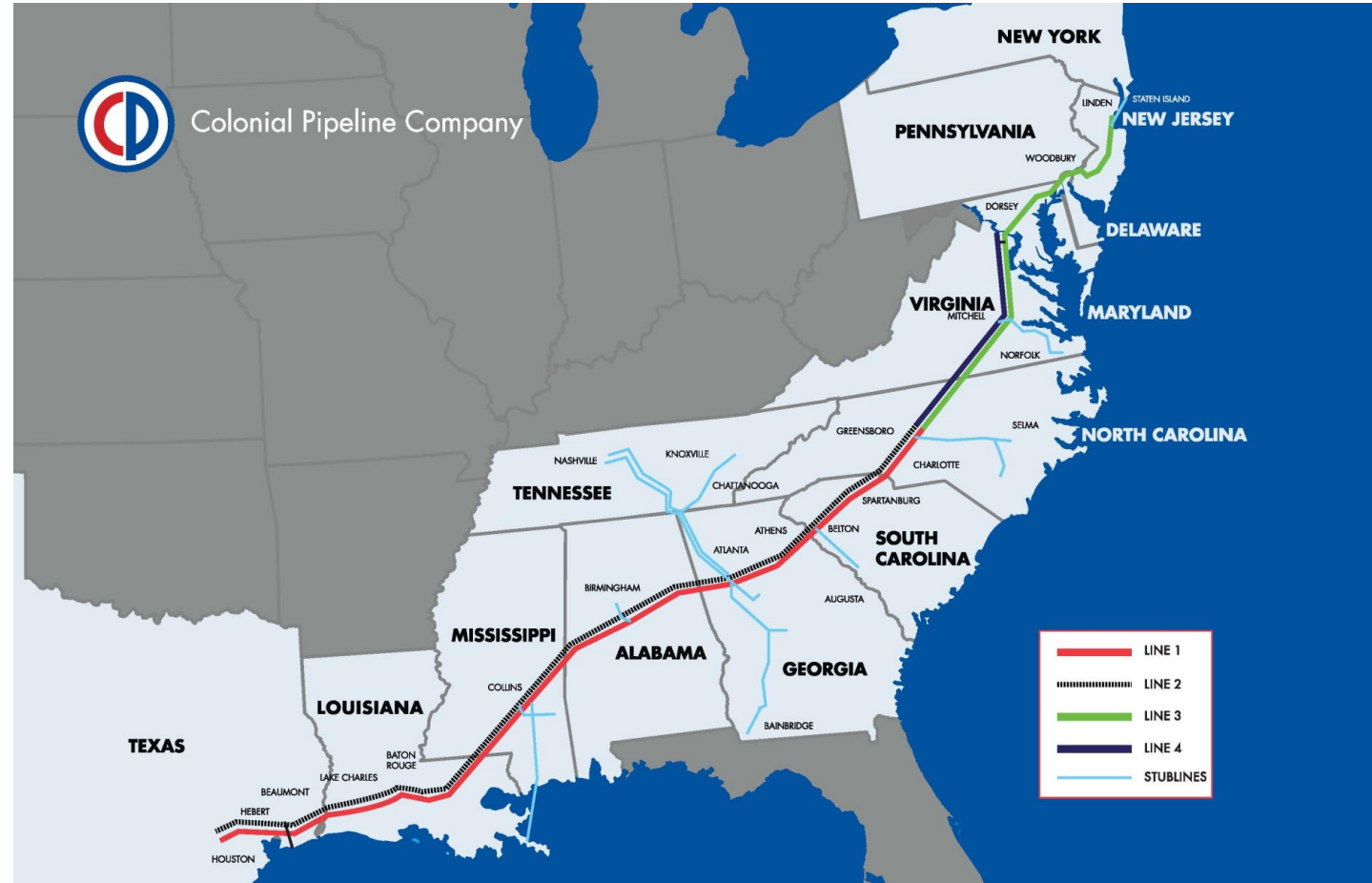
Response/Recovery

- Systems taken offline to prevent further damage and contain the spread of the ransomware attack
- Cybersecurity Firm FireEye was contacted to investigate cyber attack and help bring systems back up
- Law Enforcement and Federal Government Agencies Notified of attack
- State of Emergency Declared



Response/Recovery

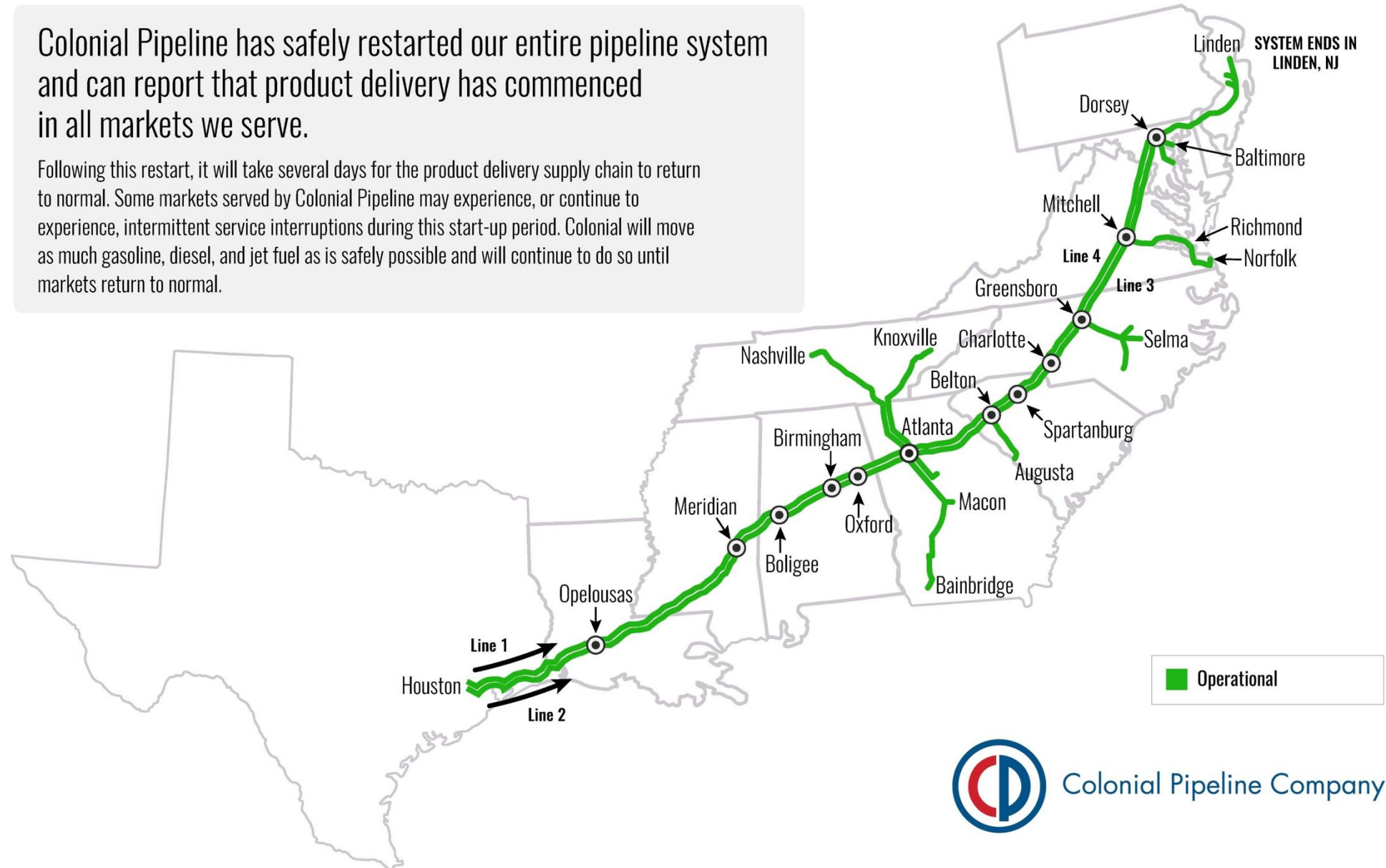
- State of Emergency Declaration led to the immediate transportation and movement of up to 29,000 miles of fuel supply delivery to affected states and restriction limit were lifted
- \$4.4 Million paid in Bitcoin hackers and Decryption Key was provided to unlock encrypted files
- System restart plan was created to bring back all affected pipelines up and running safely again
- May 7th – Colonial Pipeline performed system restart of their systems



Response/Recovery

Colonial Pipeline has safely restarted our entire pipeline system and can report that product delivery has commenced in all markets we serve.

Following this restart, it will take several days for the product delivery supply chain to return to normal. Some markets served by Colonial Pipeline may experience, or continue to experience, intermittent service interruptions during this start-up period. Colonial will move as much gasoline, diesel, and jet fuel as is safely possible and will continue to do so until markets return to normal.



Prevention

- Destroy Legacy Credentials, rebuild access controls from scratch, continuous validation on system controls, record retention (Store data for a specific amount of time, archive or destroy them!) - Spider web effect
- Multi-Factor Authentication, Designated Cybersecurity coordinator within the company
- NIST Frameworks, Access Control Frameworks, This NIST SP 800-53 database represents the controls defined in NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

TABLE 3-1: ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	Policy and Procedures	x	x	x	x
AC-2	Account Management		x	x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			x	x
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			x	x
AC-2(3)	DISABLE ACCOUNTS			x	x
AC-2(4)	AUTOMATED AUDIT ACTIONS			x	x
AC-2(5)	INACTIVITY LOGOUT			x	x
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT				
AC-2(7)	PRIVILEGED USER ACCOUNTS				
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT				
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS				

SP 800-53 Rev 5.1 and SP 800-53B Latest Versions

Control Families

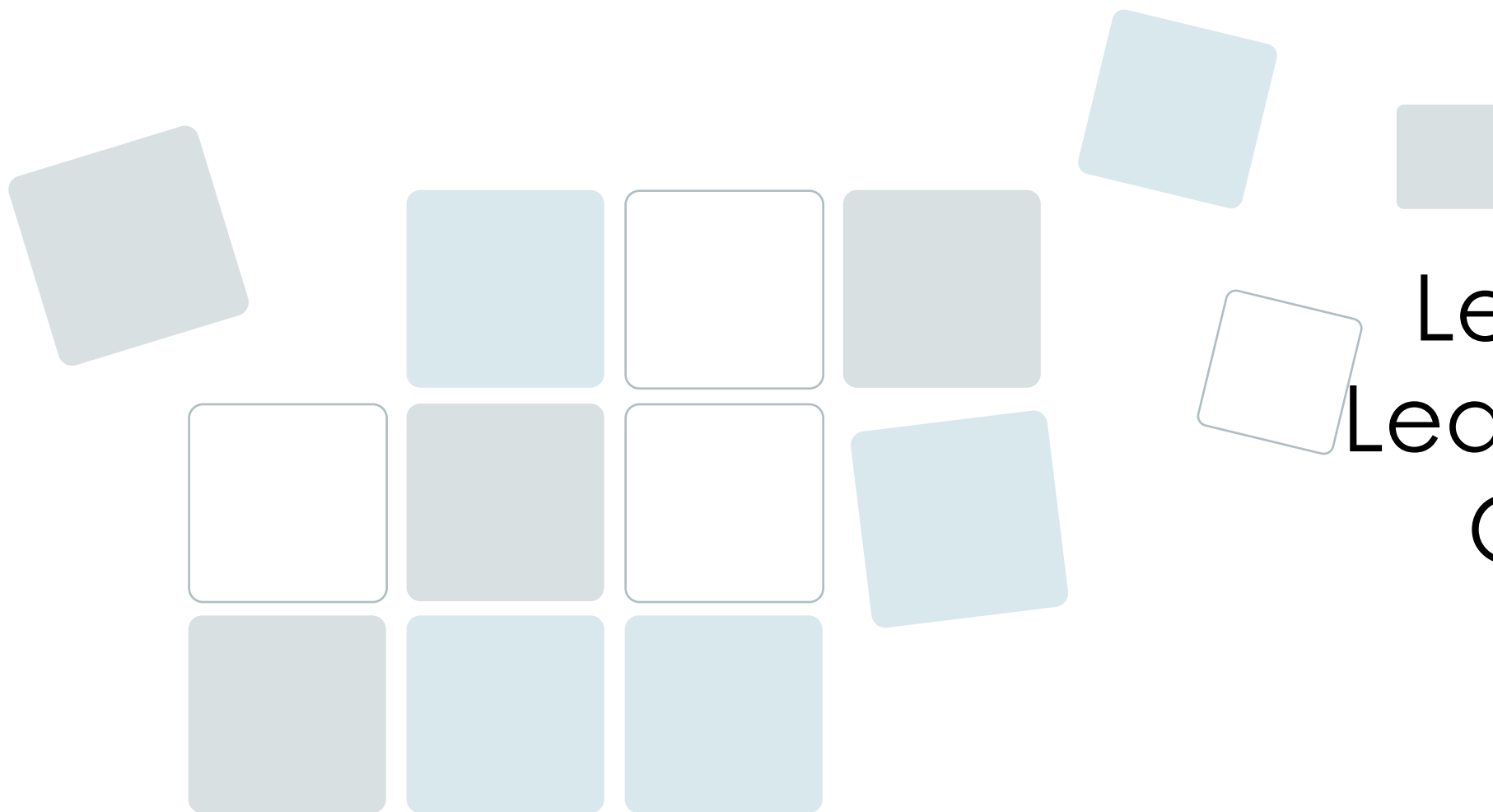
- [AC - ACCESS CONTROL](#)
- [AT - AWARENESS AND TRAINING](#)
- [AU - AUDIT AND ACCOUNTABILITY](#)
- [CA - ASSESSMENT, AUTHORIZATION, AND MONITORING](#)
- [CM - CONFIGURATION MANAGEMENT](#)
- [CP - CONTINGENCY PLANNING](#)
- [IA - IDENTIFICATION AND AUTHENTICATION](#)
- [IR - INCIDENT RESPONSE](#)
- [MA - MAINTENANCE](#)
- [MP - MEDIA PROTECTION](#)
- [PE - PHYSICAL AND ENVIRONMENTAL PROTECTION](#)
- [PL - PLANNING](#)
- [PM - PROGRAM MANAGEMENT](#)
- [PS - PERSONNEL SECURITY](#)
- [PT - PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY](#)
- [RA - RISK ASSESSMENT](#)
- [SA - SYSTEM AND SERVICES ACQUISITION](#)
- [SC - SYSTEM AND COMMUNICATIONS PROTECTION](#)
- [SI - SYSTEM AND INFORMATION INTEGRITY](#)
- [SR - SUPPLY CHAIN RISK MANAGEMENT](#)

Jump To:

- [REVISION 5.1](#)
- [Home](#)
- [Control Families](#)
- [Low-Impact](#)
- [Moderate-Impact](#)
- [High-Impact](#)
- [Privacy Control Baseline](#)
- [All Controls](#)
- [Search](#)

Preparedness

- Review current cybersecurity defenses, perform risk assessments to identify vulnerabilities and how those known vulnerabilities can impact their systems
- Have a cybersecurity coordinator, review current activities on recommendations made on identified cyber risks and identified security gaps to develop remediation measures
- Develop a business continuity plan
- Check the box exercises, hiring third-party cybersecurity consultants to review cybersecurity posture
- Notify Law Enforcement and Government Agencies as soon as possible



Lessons Learned & Q&A

Lessons Learned

- Notify Law Enforcement and Government Agencies as soon as possible
- Recognize the complexity of Information Technology (IT) and Operational Technology (OT) and how it's interconnected
- Don't pay for ransomware attacks, Payment for a ransomware attack can lead up to more cyber-attacks creating a ripple effect where they are constantly being targeted.
- Look for legacy entries into the system that don't have multi factor authentication