COLORADO

Division of Homeland Security
& Emergency Management

Department of Public Safety

LESSONS IN RESILIENCY

WHAT THE RANSOMWARE ATTACK ON COLORADO'S DEPARTMENT OF TRANSPORTATION TAUGHT US

MICHAEL WILLIS

DIRECTOR, COLORADO OFFICE OF
EMERGENCY MANAGEMENT

TOPICS

- How It Happened
- What It Did
- How We Responded
- What it Didn’t Do
- How Resiliency Made a Difference
  - Before the Attack
  - During the Attack
  - After the Attack
- Sunshine and Roses?

HOW IT HAPPENED

CDOT brought a virtual server

Nothing wrong w

Virtual server conn

N

Virtu

??

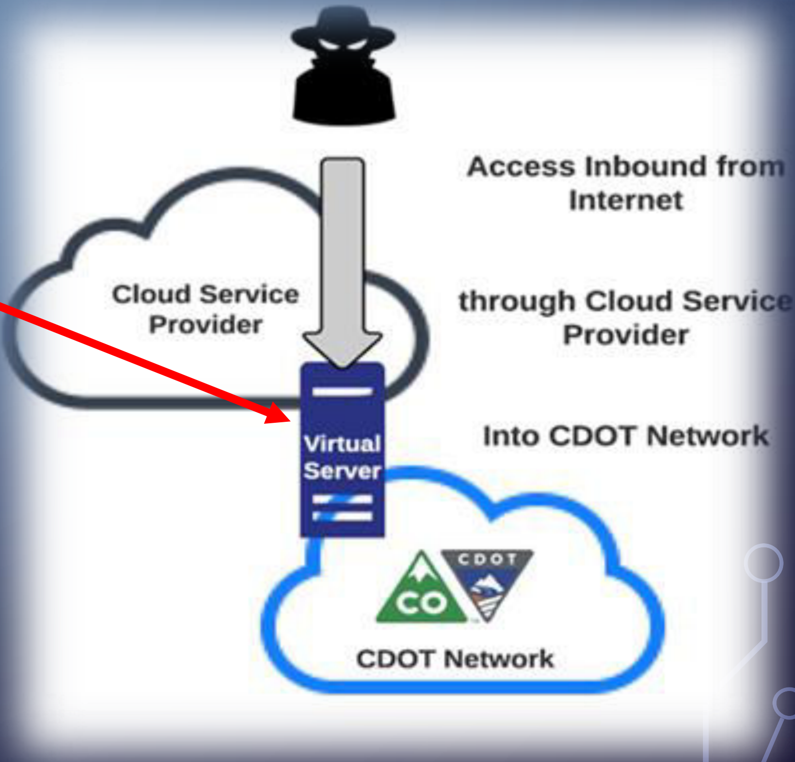
t have standard security controls

Uh-oh

ablished as domain administrator account

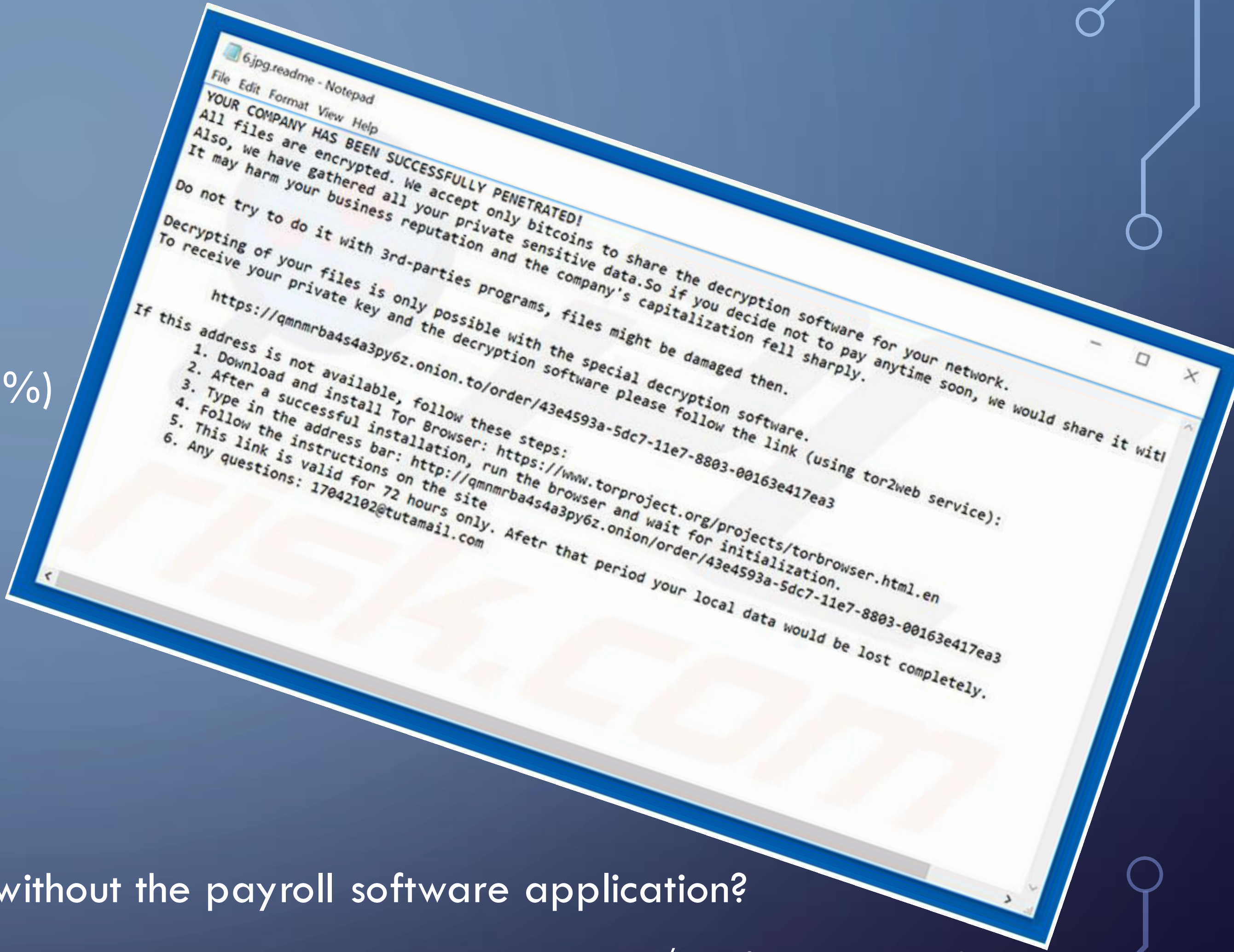
OH #$%&

Brute force attack began the day the server was brought online. Over 40,000 brute force password attempts were made. System was compromised within 48 hours



WHAT IT DID

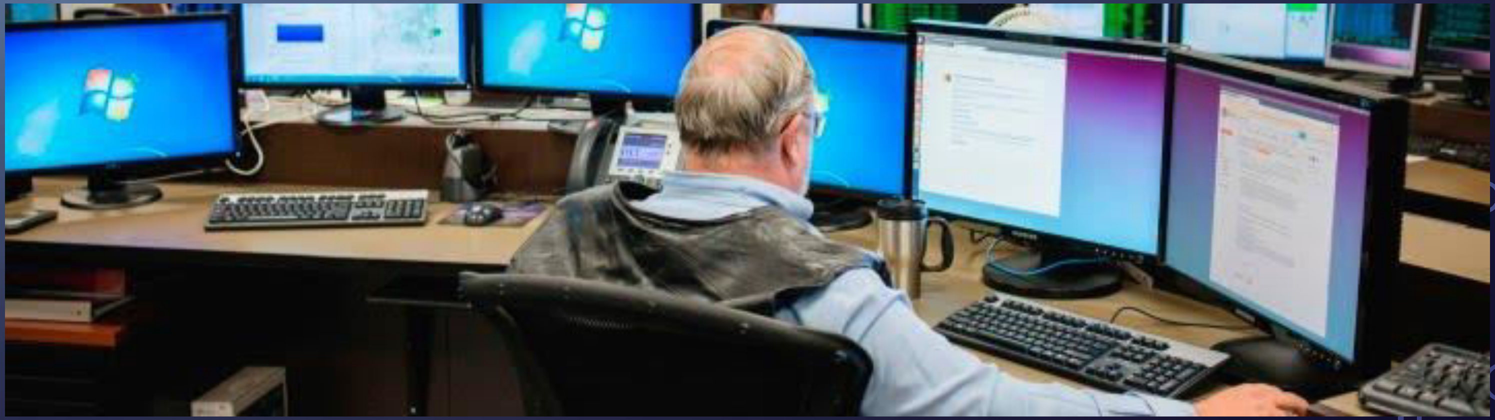
- Equipment
  - 1274 laptops (39%) and 427 desktops (81%)
  - 339 servers
  - 158 databases
  - 154 software applications
  - All VoIP phones
- Consider:
  - How do you pay employees & contractors without the payroll software application?
  - How do you communicate with internal and external stakeholders without email/conference call?
  - What do you tell external contractors when you disconnect them from your network?



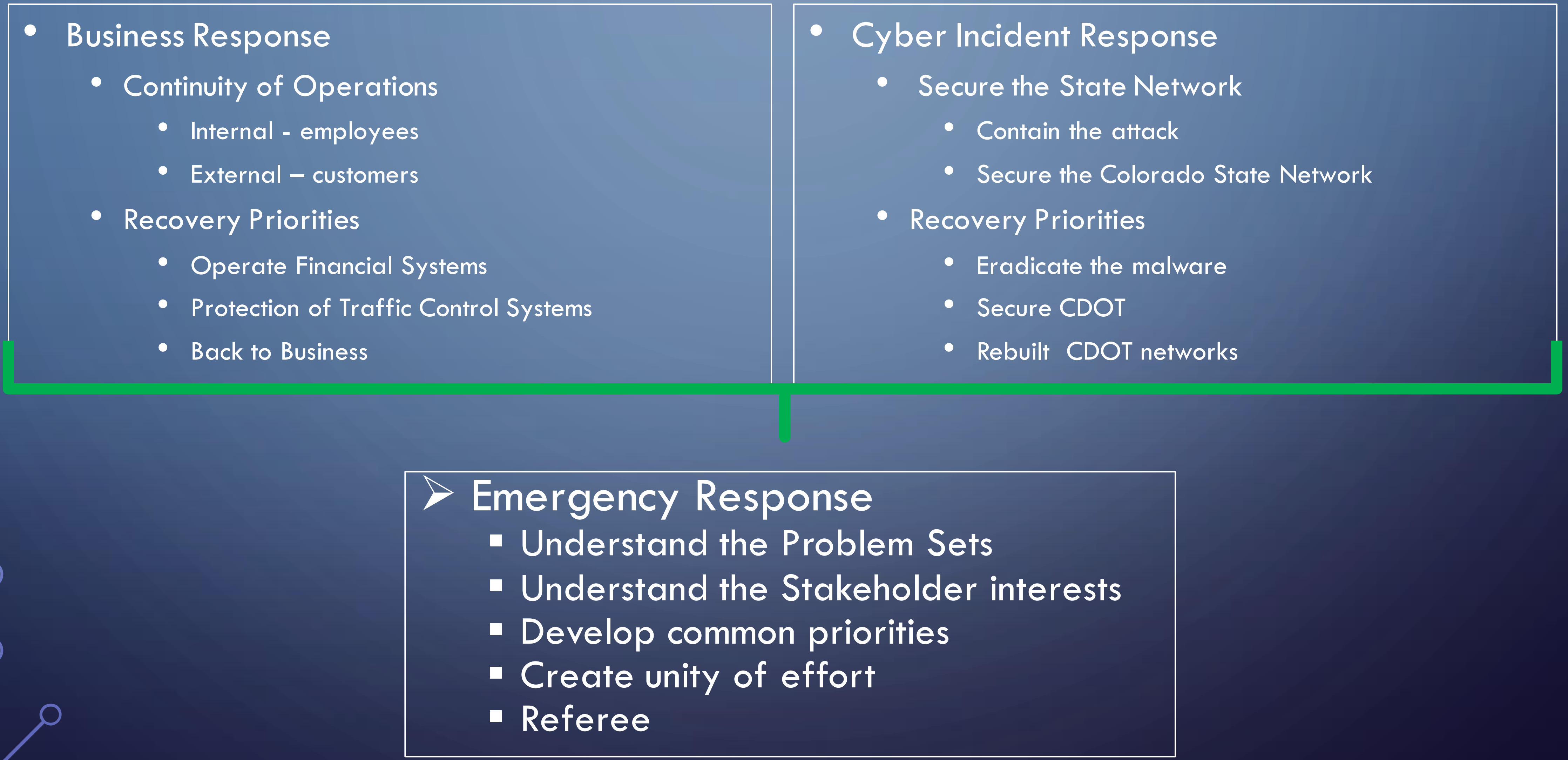
```
YOUR COMPANY HAS BEEN SUCCESSFULLY PENETRATED!
All files are encrypted. We accept only bitcoins to share the decryption software for your network.
Also, we have gathered all your private sensitive data.So if you decide not to pay anytime soon, we would share it wit
It may harm your business reputation and the company's capitalization fell sharply.
Do not try to do it with 3rd-parties programs, files might be damaged then.
Decrypting of your files is only possible with the special decryption software.
To receive your private key and the decryption software please follow the link (using tor2web service):
        https://qmnmrba4s4a3py6z.onion.to/order/43e4593a-5dc7-11e7-8803-00163e417ea3
If this address is not available, follow these steps:
   1. Download and install Tor Browser: https://www.torproject.org/projects/torbrowser.html.en
   2. After a successful installation, run the browser and wait for initialization.
   3. Type in the address bar: http://qmnmrba4s4a3py6z.onion/order/43e4593a-5dc7-11e7-8803-00163e417ea3
   4. Follow the instructions on the site
   5. This link is valid for 72 hours only. Afetr that period your local data would be lost completely.
   6. Any questions: 17042102@tutamail.com
```

WHAT IT DIDN'T DO

- It didn't shut down transportation in Colorado
- It didn't put the public at risk
- It didn't break containment or infect any other network
- It didn't undermine public confidence
- It didn't have lasting negative impacts
    - We're better now than we were before!
- It didn't get anyone fired



HOW WE RESPONDED



- Business Response
  - Continuity of Operations
    - Internal - employees
    - External – customers
  - Recovery Priorities
    - Operate Financial Systems
    - Protection of Traffic Control Systems
    - Back to Business

- Cyber Incident Response
  - Secure the State Network
    - Contain the attack
    - Secure the Colorado State Network
  - Recovery Priorities
    - Eradicate the malware
    - Secure CDOT
    - Rebuilt CDOT networks

- ➢ Emergency Response
  - ▪ Understand the Problem Sets
  - ▪ Understand the Stakeholder interests
  - ▪ Develop common priorities
  - ▪ Create unity of effort
  - ▪ Referee

HOW RESILIENCY MADE A DIFFERENCE
BEFORE THE ATTACK

- Secure Backup “Backup Colorado”
- Network Segmentation
- Exercises with Governor’s Office of Information Technology, Colorado National Guard, Office of Emergency Management & Academia
  - Senior Leader Engagement: CISO, GO, Director

HOW RESILIENCY MADE A DIFFERENCE DURING THE ATTACK

- Execution of CDOT's Continuity of Operations Plan
- Good public information plan
- Emergency management discipline
- Personnel care
  - Rest
  - Diet
  - Climate
  - Relief (EMAC)

HOW RESILIENCY MADE A DIFFERENCE AFTER THE ATTACK

- Created a “call for action”
  - Legislative support
    - ~$12m
  - Agency support
    - “Don’t let that happen to us!”
- Improved tools
  - Two-factor authentication
  - Instruction detection systems
  - Upgraded firewalls
  - Reduced privileged administrator accounts
- Improved response plans
  - Better contracts with vendors
  - Institutionalized relationships between agencies

SUNSHINE & ROSES???

WHAT MADE US LESS RESILIENT

- Turnover and lack of firewall personnel
- Delayed implementation of updated firewalls
- Outdated systems in use
- Lack of good network diagrams
- Incomplete security guidance & lack of discipline
- Exercises that didn’t include all stakeholders

KEY TAKEAWAYS

- Define your Cyber Incident Response Team
  - Exactly who does exactly what??
    - Network team
    - Malware team
    - Endpoint team
  - Rehearse (no really – rehearse…)
- Seriously address Cyber in your COOP
  - Holistic approach - not just an IT problem
  - What's at risk? What will you do?
  - CDOT Senior Executive "Our COOP was better suited for a meteor hit than a cyber attack"
- Do cyber response exercises that include Cyber Emergency Management and Business responses
- Mitigate. You mitigate for other risks, so do it for this one
- It's an incident – act like it!
  - P.S. don't freak out – it's an incident, you've done this before
- Public Information Officers matter!

COLORADO

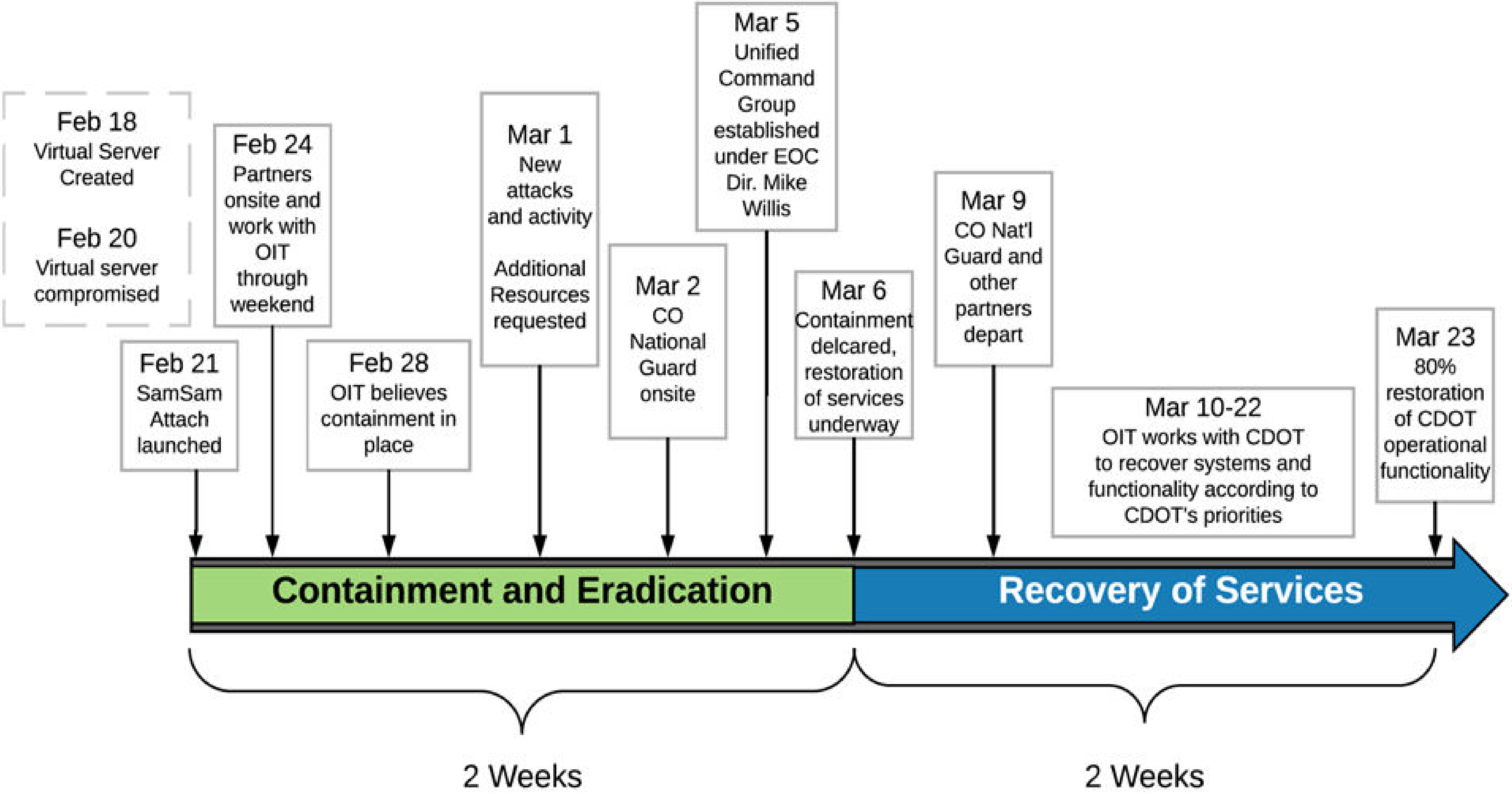
Division of Homeland Security
& Emergency Management

Department of Public Safety

QUESTIONS?

Michael Willis
Director, Office of Emergency Management
Mike.willis@state.co.us
720-852-6694

BACKUP SLIDES



Feb 18 Virtual Server Created

Feb 20 Virtual server compromised

Feb 21 SamSam Attach launched

Feb 24 Partners onsite and work with OIT through weekend

Feb 28 OIT believes containment in place

Mar 1 New attacks and activity

Additional Resources requested

Mar 2 CO National Guard onsite

Mar 5 Unified Command Group established under EOC Dir. Mike Willis

Mar 6 Containment delcared, restoration of services underway

Mar 9 CO Nat'l Guard and other partners depart

Mar 10-22 OIT works with CDOT to recover systems and functionality according to CDOT's priorities

Mar 23 80% restoration of CDOT operational functionality

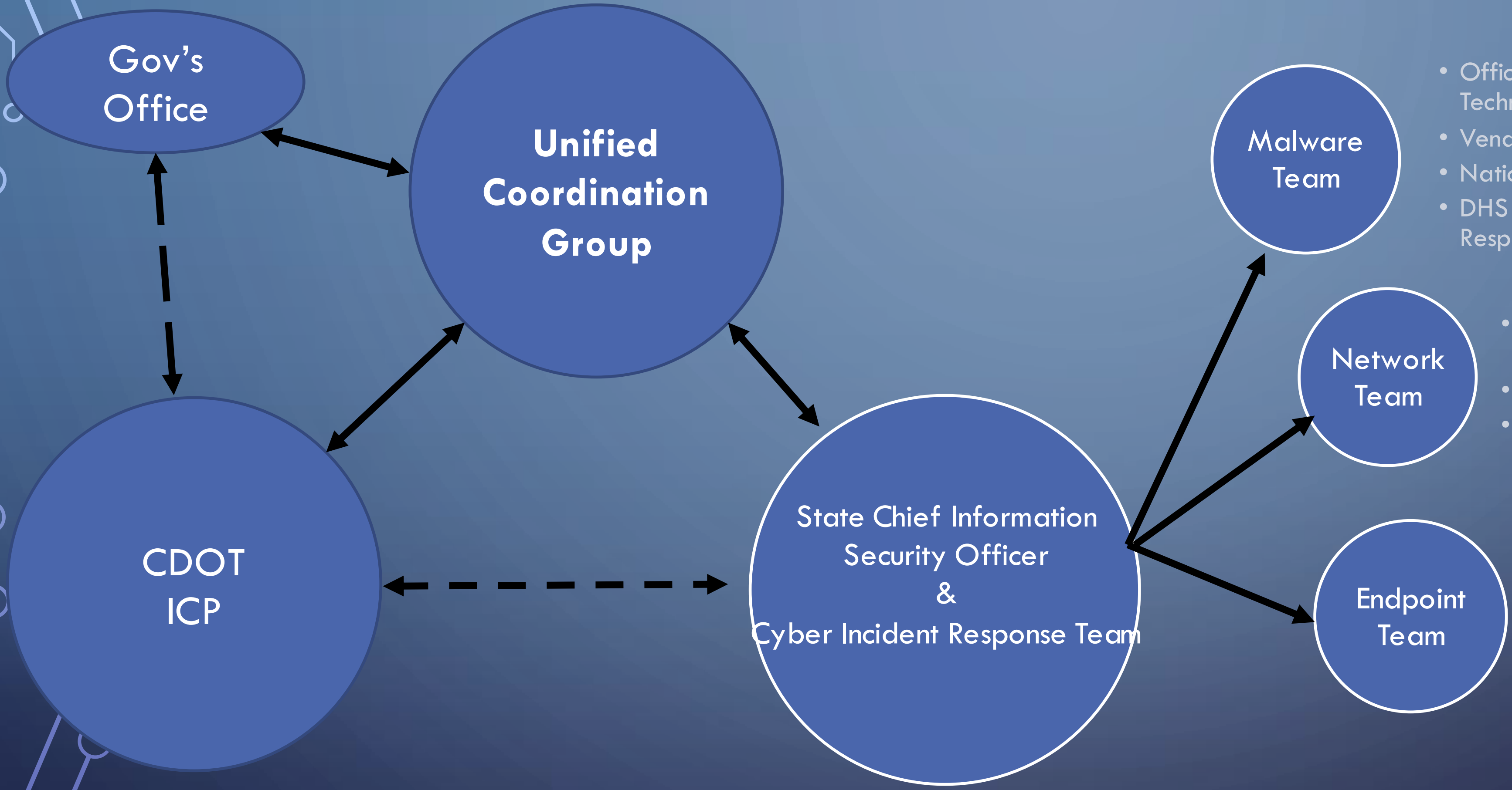
Containment and Eradication

Recovery of Services

2 Weeks

2 Weeks

THE CYBER PLAYERS (AS DESIGNED(ISH))



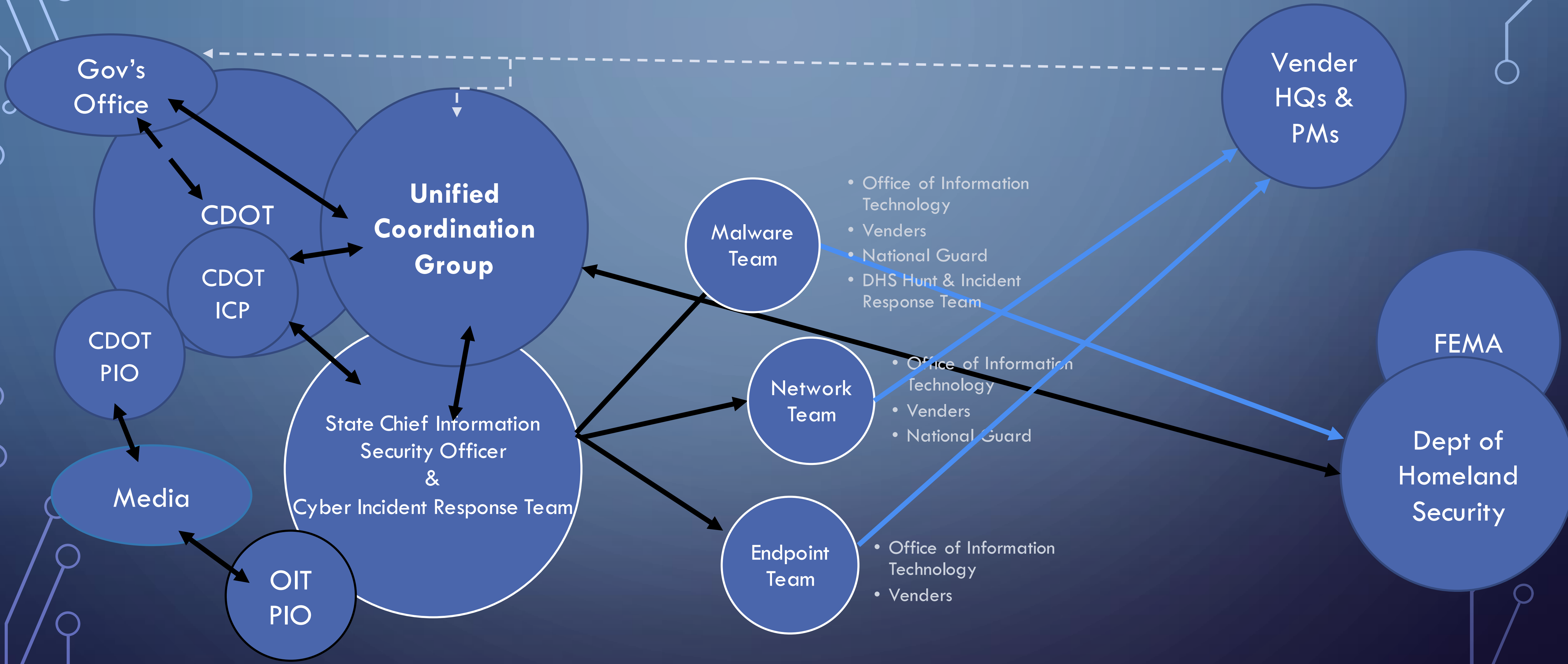
Gov's Office
Unified Coordination Group
CDOT ICP
State Chief Information Security Officer & Cyber Incident Response Team
Malware Team
Network Team
Endpoint Team

- Office of Information Technology
- Venders
- National Guard
- DHS Hunt & Incident Response Team

- Office of Information Technology
- Venders
- National Guard

- Office of Information Technology
- Venders

THE CYBER PLAYERS (WHAT REALLY HAPPENED(ISH)



Gov's Office

CDOT

CDOT ICP

Unified Coordination Group

CDOT PIO

Media

OIT PIO

State Chief Information Security Officer & Cyber Incident Response Team

Malware Team

- Office of Information Technology
- Venders
- National Guard
- DHS Hunt & Incident Response Team

Network Team

- Office of Information Technology
- Venders
- National Guard

Endpoint Team

- Office of Information Technology
- Venders

Vender HQs & PMs

FEMA

Dept of Homeland Security

WHAT WE'D DO DIFFERENTLY

- Deploy Incident Command (Unified Command Group) sooner
- Define lanes and organized by tasks sooner
- Clarify lanes and roles with vendors sooner
- Synchronize the operational rhythms sooner (CDOT, Cyber Response, UCG)
- Stop chasing the bad guy sooner

WHAT WE'D DO AGAIN

- Coordinate the external message
- Issue an EMAC to rest tired IT personnel
- Call in Office of Emergency Management for logistics coordination
  - How do you feed a roomful of hungry people when they are sick of pizza?
  - How do you keep track of who your responders were?
- Establish priorities early and post priorities on the wall to remind responders of the goals