What We Learned

Key Takeaways from the 2018 Ransomware Attack on Colorado Department of Transportation

February – March 2018

Michael Willis

Colorado Director of Emergency Management

Topics

- How It Happened
- What It Did
- Timeline
- How We Responded
  - Business Response
  - Cyber Incident Response
  - Emergency Response
- The Cyber Players
- What We'd Do Differently
- **Key Takeaways**

Credits

- Debbi Blyth
  - Chief Information Security Officer

- Kevin Klein
  - Director, Division of Homeland Security and Emergency Management

How It Happened

CDOT brought a virtual server o

Nothing wrong wit

Virtual server conn

Not

Virtu

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

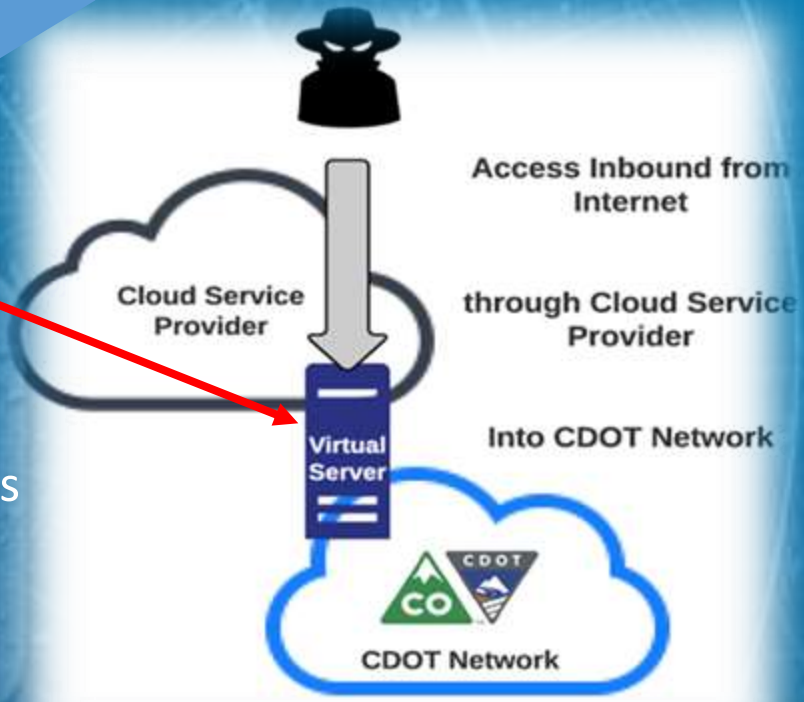
??

t have standard security controls

Uh-oh

tablished as domain administrator account

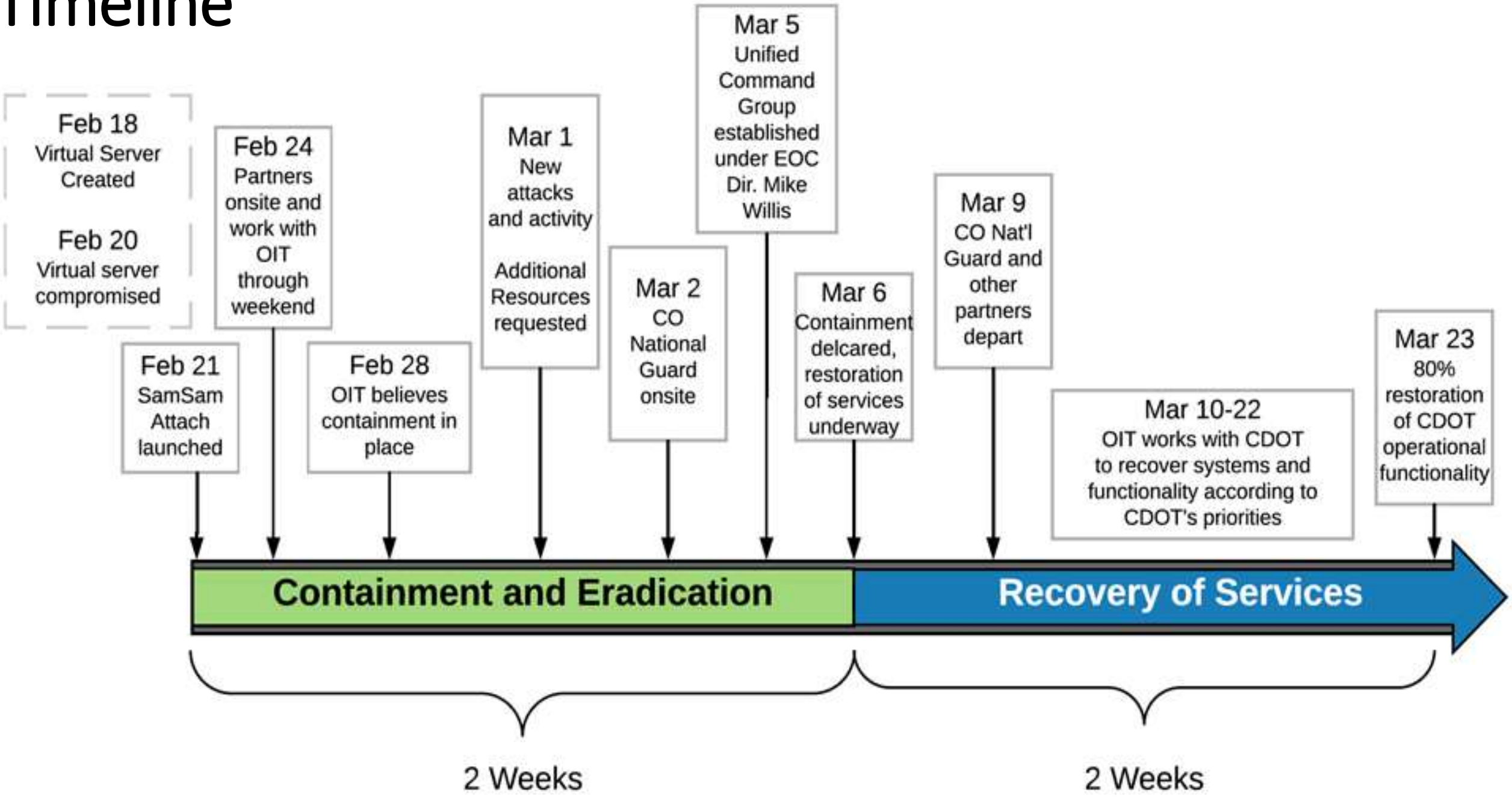
OH #$%&



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?

Timeline


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

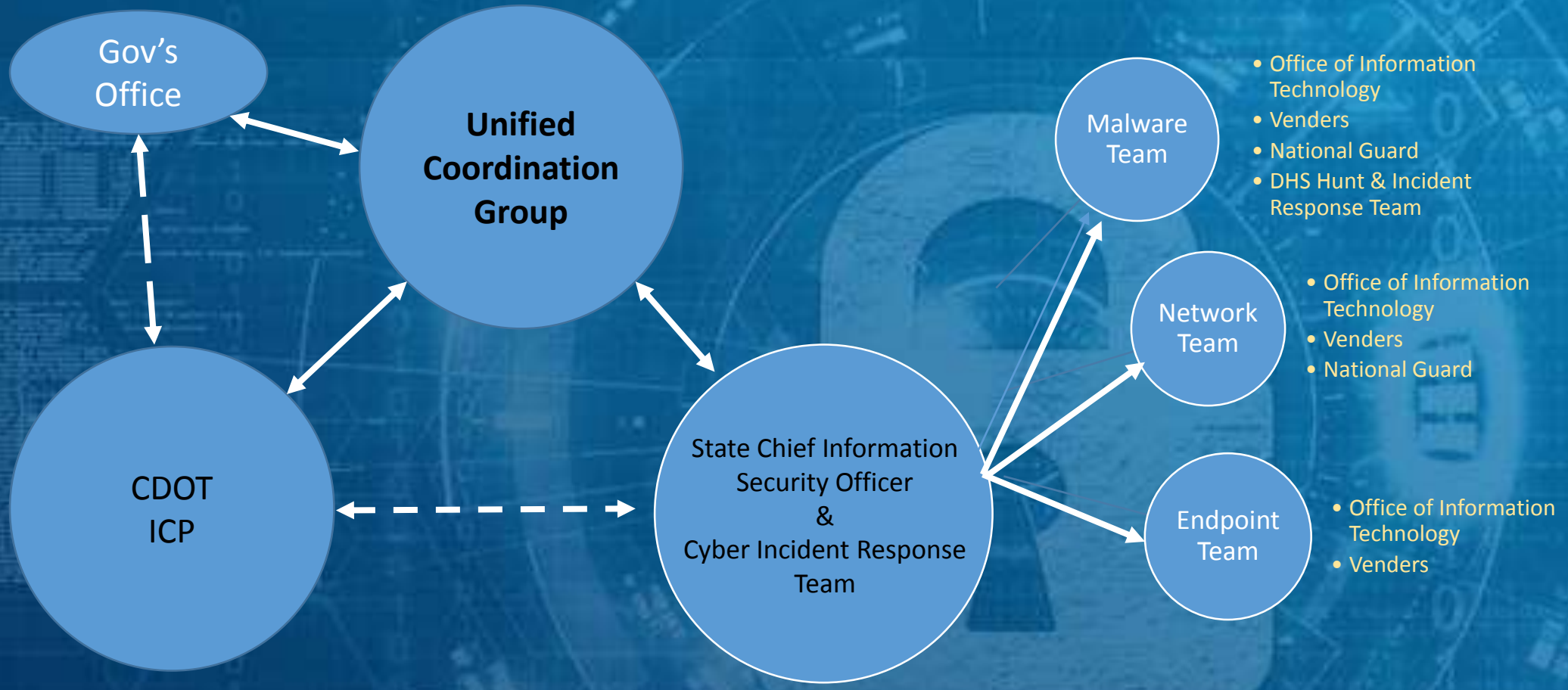
How We Responded

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

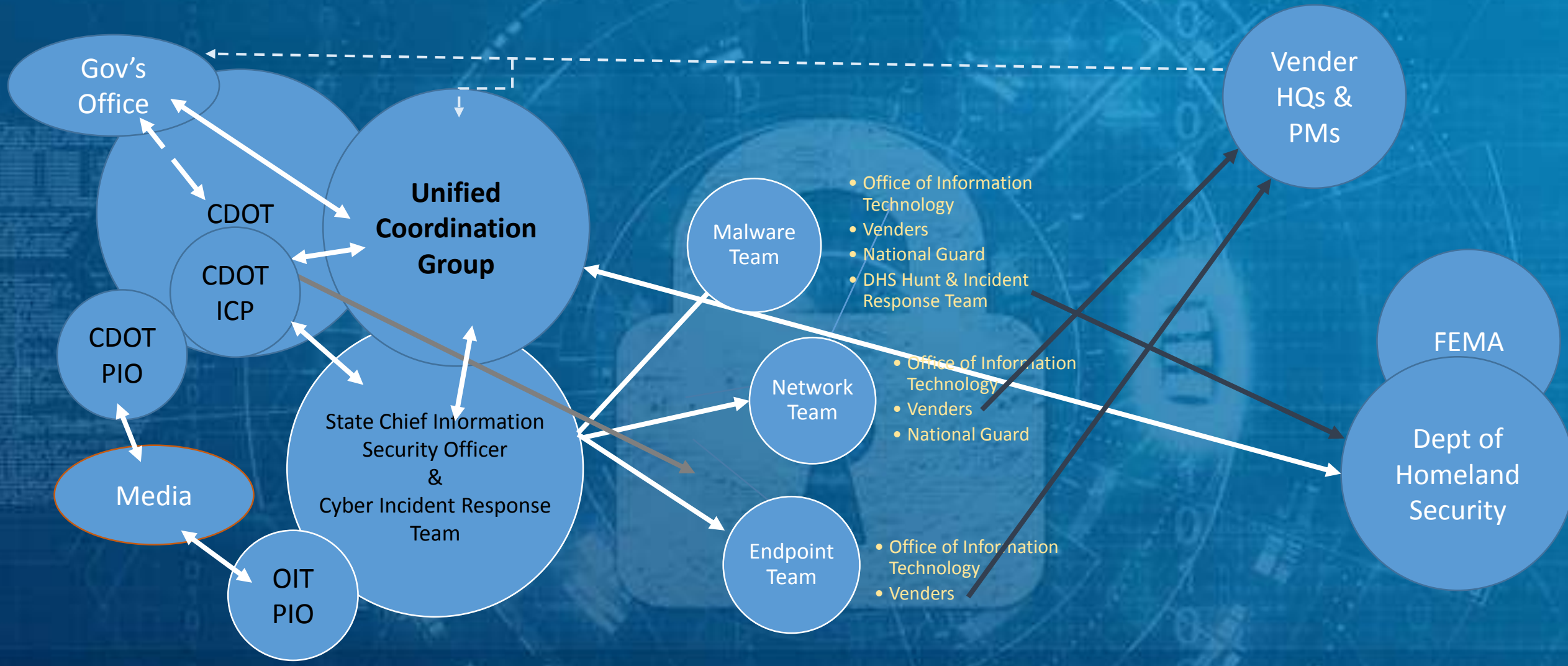
- **Cyber Incident Response**
  - Secure the State Network
    - Contain the attack
    - Secure the Colorado State Network
  - Recovery Priorities
    - Eradicate the malware
    - Secure CDOT
    - Rebuilt CDOT networks

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

The Cyber Players (as designed(ish))



The Cyber Players (what really happened(ish)



Firsts

- Cybersecurity state disaster declaration
- National Guard cyber incident deployment
- FEMA cybersecurity mission
  - Mobile Emergency Response Support (MERS) Vehicle
- EMAC for a cybersecurity mission
- DHS HIRT deployment (Hunt and Incident Response Team)


Patching Step


2
the investigation and gathering evidence
Prioritize handling the incident based on the
impact, recoverability effort, etc.)
3
Report the incident to the
4

Why a State Declaration Helped

- Sent the message that this was not just an Office of Technology problem, it was a State problem
- Enabled unified effort to address both the virtual impacts and the physical world consequences with a synchronized approach
- Set the conditions for federal assistance without a Stafford Act declaration
- Allowed for the use of the Colorado National Guard
- Enabled use of the Emergency Management Assistance Compact (EMAC)

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

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
  - Secure backup = mitigation
- 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!

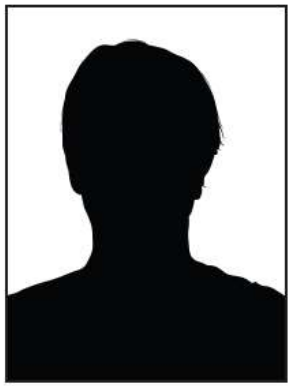
Epilogue

WANTED BY THE FBI

SAMSAM SUBJECTS

Conspiracy to Commit Fraud and Related Activity in Connection with Computers; Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer; Transmitting a Demand in Relation to Damaging a Protected Computer

Mohammad Mehdi Shah Mansouri



Faramarz Shahi Savandi

RECEIVED
NOV 26 2018
AT 8:30 M
WILLIAM T. WALSH, CLERK

JSH/WAH/2016R00103

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Criminal No. 18 - CR - 704 (BRM)
	:	
FARAMARZ SHAHI SAVANDI and	:	18 U.S.C. § 371
MOHAMMAD MEHDI SHAH	:	18 U.S.C. § 1030(a)(5)(A)
MANSOURI	:	18 U.S.C. § 1030(a)(7)(C)
	:	18 U.S.C. § 1349

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark,

harges:

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

1. At all times relevant to Count 1 of this Indictment:

The Defendants

a. Defendant FARAMARZ SHAHI SAVANDI was a computer

acker who resided in Iran.

b. Defendant MOHAMMAD MEHDI SHAH MANSOURI was a

computer hacker who resided in Iran.

RECOVERY

CONTAINMENT

2018

ERADICATION

SUSTAIN