ODOT Critical Cyber Incident Overview

Ben Gherezgiher, State Chief Information Security Officer

Joint Committee on Information Management and Technology

September 27, 2023

ENTERPRISE information services

Agenda

- Global Cybersecurity Threat Overview
- Types of Cyber Incidents
- Critical Cyber Incident Management Protocols
- Cyber Incident # CSS20230603A Overview
- Questions & Answers

ENTERPRISE information services

Global Cybersecurity Threat Landscape

CYBER THREAT ACTOR		MOTIVATION	
NATION STATES		GEOPOLITICAL	Political / military gain etc.
CYBERCRIMINALS		PROFIT	Organized for monetary gain etc.
HACKTIVISTS		IDEOLOGICAL	Political etc.
TERRORISTS		IDEOLOGICAL VIOLENCE	Ideological, religious, political etc.
THRILL SEEKERS		SATISFACTION	Nuts/crazy
INSIDER THREAT		DISCONTENT	Or can be planted for industrial espionage

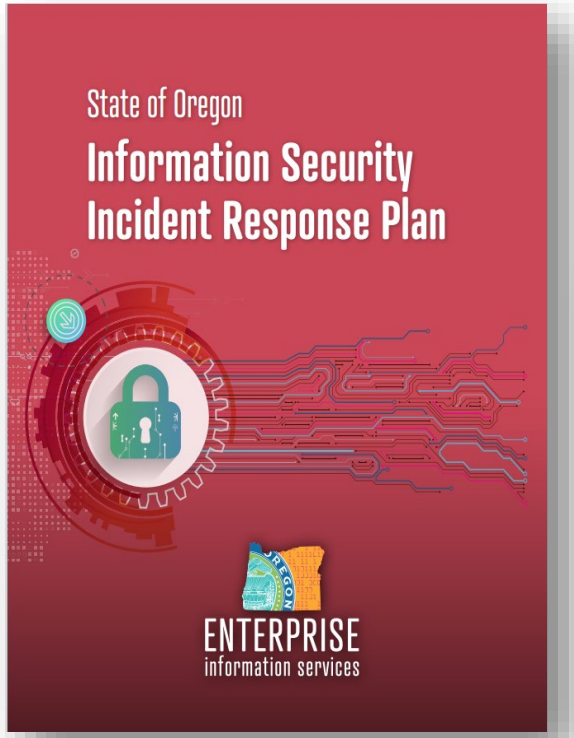
ENTERPRISE information services

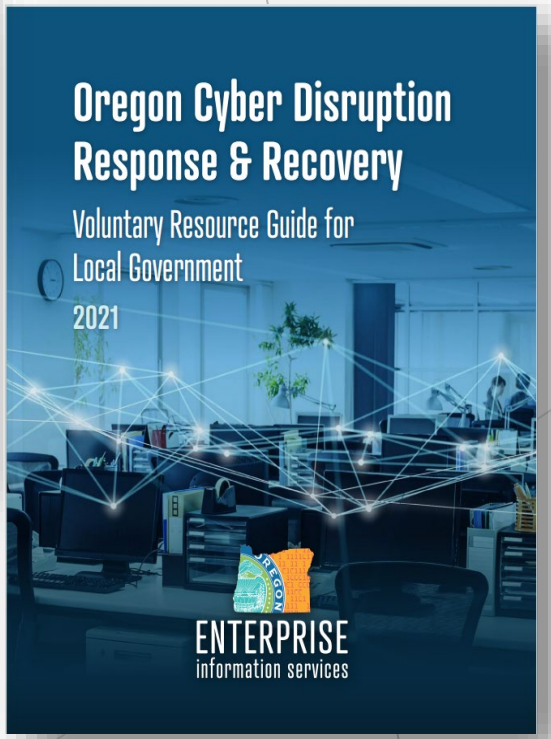
Global Impact: MOVEit Data Breach

- As of August 31, 2023, over 1,000 organizations and 60 million individuals affected worldwide.
- US based organizations accounted for 84.7%, Germany 3.4%, Canada 2.6%, and UK 1.9%, according to analysis provided by Emsisoft.
- According to IBM's "Cost of data breach report 2023", third party supply chain compromises cost 11.8% higher and take 12.8% longer to identify and contain than other types of data breaches.

Types of Cyber Incidents – General

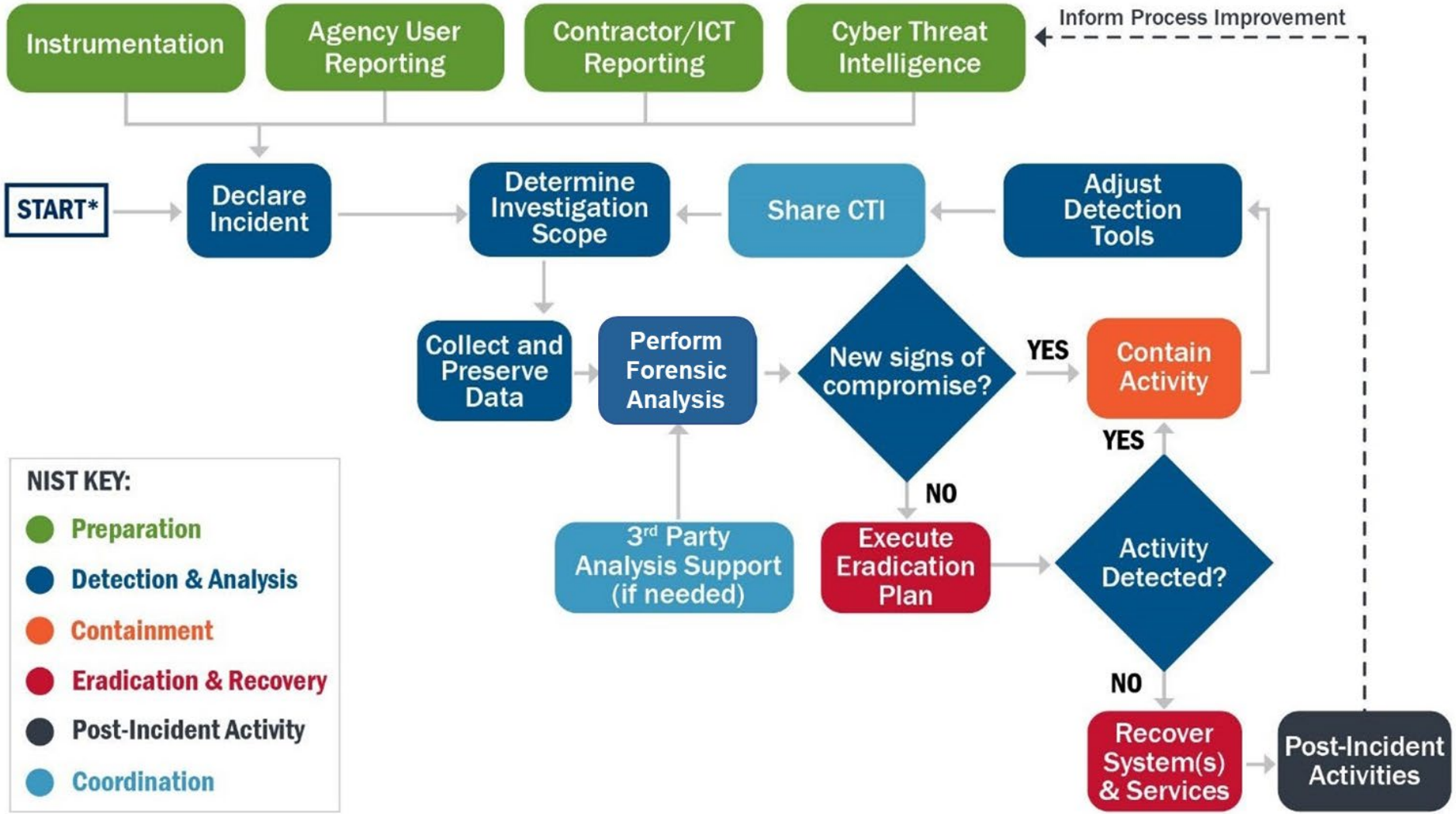
- Information Security Incident Response Plan
- Levels of escalation and incident communication planning check lists
- Cyber Disruption Response Plan
- FEMA ICS disaster vs cyber disaster





ENTERPRISE information services

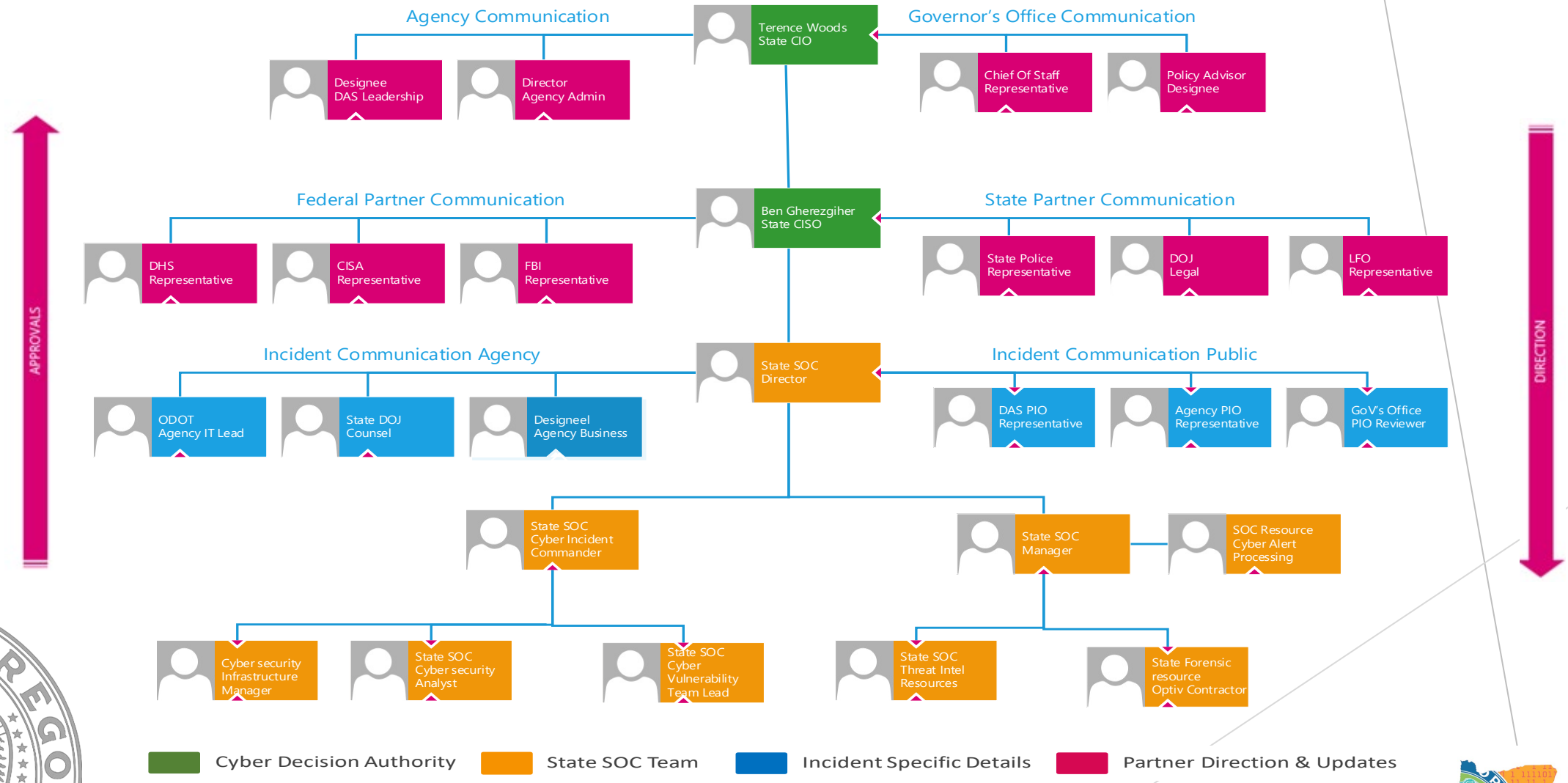
Cyber Incident Processing Workflow - General



CTI: Cyber Threat Indicator

ENTERPRISE information services

Cyber Incident Communication & Command Structure



ENTERPRISE information services

Cyber Incident: #CSS20230603A (MOVEit) Overview

Attack Disclosures

- **MOVEit** is a file transfer business application mostly used as an ETL (extract, transform, load) tool to transfer data among systems. Application is developed and supported by Progress Software.
- **Zero-day** – attack that exploits vulnerability on the software code to access database and breach data.
- **Adversary** – sophisticated Russian-linked ransomware gang known as CLOP.
- **The Oregon Question:** Data has been exfiltrated from ODOT. There is very little that the agency could have done to stop zero-day attack. Staff worked diligently with EIS Cyber Security Services (CSS) and our federal partners. Software have been patched and is closely monitored; agency is working on applying CSS recommendations to further reduce risk.
- **Dark web disclosure so far:** As of September 19, 2023, CLOP did not mention anything about the state of Oregon in the dark web.

Thank you

Shirlene A Gonzalez
Legislative & Communications Director
shirlene.a.gonzalez@das.oregon.gov

ENTERPRISE
information services