ENTERPRISE
information services

# Statewide Information Security Report

Ben Gherezgiher
State Chief Information Security Officer

Joint Committee on Ways and Means
General Government Subcommittee

April 24, 2025

# Agenda

- Global Cybersecurity Industry Overview
- CSS Cyber Services Areas
- CSS Statewide Cyber Standards
- CSS Cyber Assessments
- CSS High Level Metrics
- CSS Projects and Initiatives
- CSS Cyber Awareness and Partnerships

# Global Cybersecurity Industry Overview

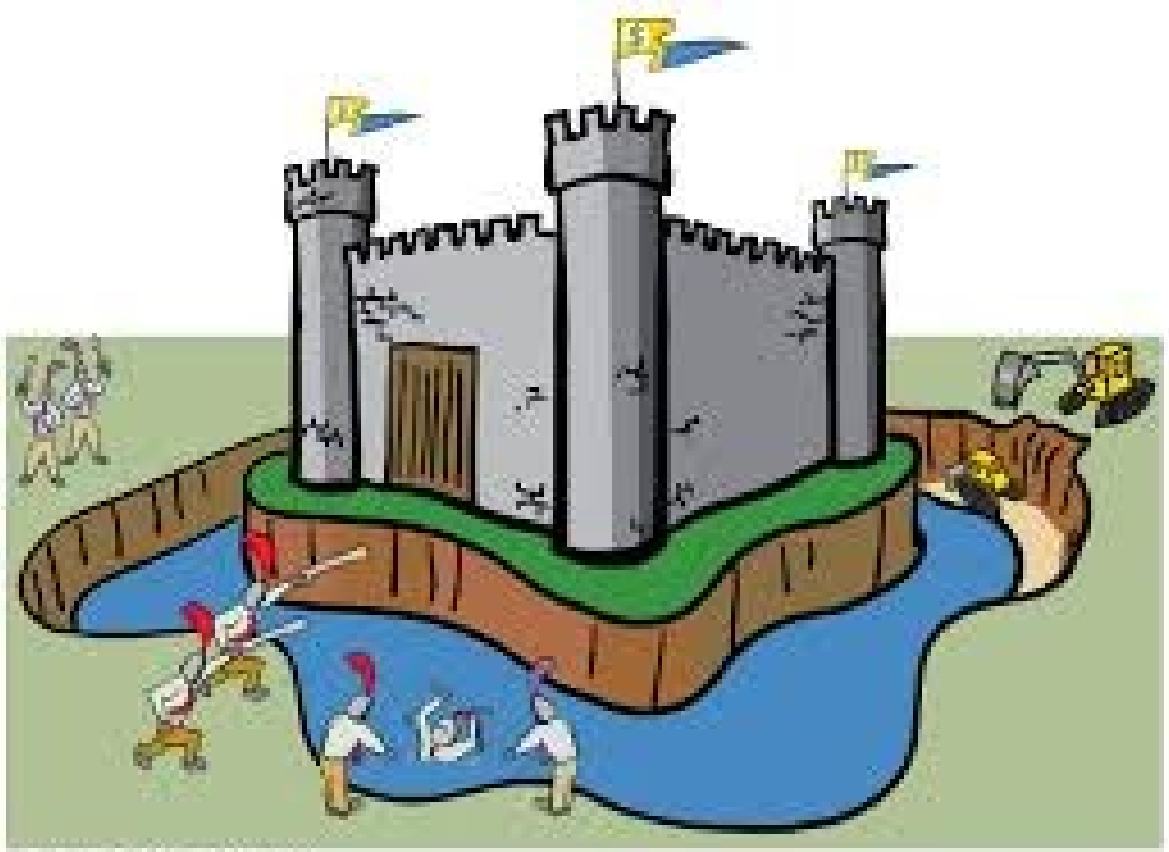


Illustration by Dennis Corporation

- The days of castle-and-moat cybersecurity strategies are gone.
- Hackers are becoming too advanced, and threats exist both inside and outside of an organization's network.
- Zero Trust security model recognizes that these threats are vulnerabilities and must be addressed.
- Whether users are internal employees or external third parties, trust must be eliminated, and verification must become the new standard.

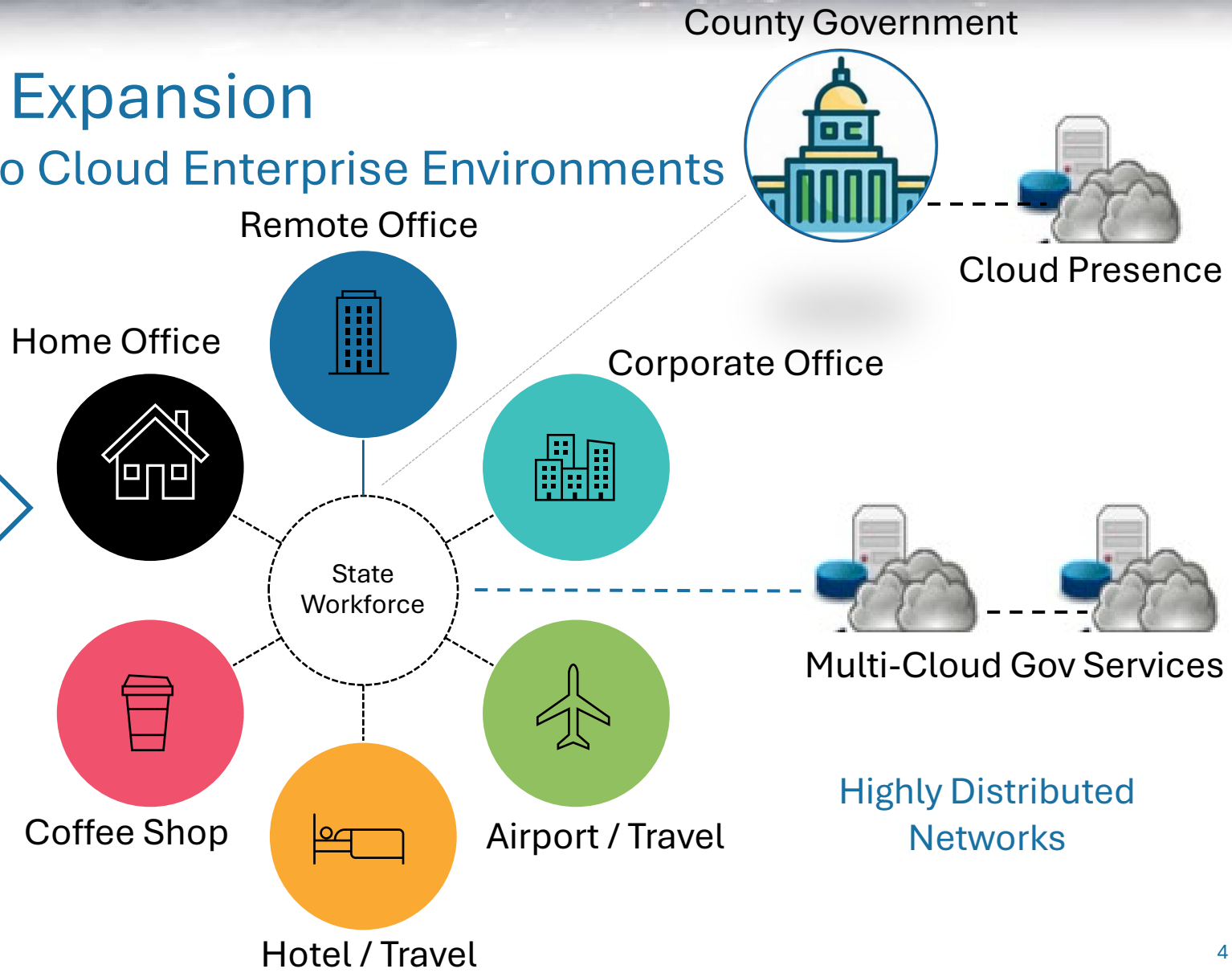
ENTERPRISE information services

# Threat Landscape Expansion

## Multi-Cloud and Cloud to Cloud Enterprise Environments

Office Workers
Localized Networks

Transition



# Global Threat Actors Overview

| | | | | | |
|---|---|---|---|---|---|
| Blizzard<br>**Russia** | Typhoon<br>**China** | Sandstorm<br>**Iran** | Sleet<br>**North Korea** | Dust<br>**Turkey** | Cyclone<br>**Vietnam** |
| Rain<br>**Lebanon** | Hail<br>**South Korea** | Tempest<br>**Financially motivated** | Tsunami<br>**Private sector offensive actor** | Flood<br>**Influence operations** | Storm<br>**Groups in development** |

- Additionally: Clop cyber gang, AlphaV, Royal cyber gang

# Global Threat Actors Overview

## Threat Actor High Level Classification

**Nation-State**

**Goals:** National strategic, economic, and security
**Activity:** Typically, espionage

**Ability Characteristics:**
At times sophisticated, specialized
Capable of intentional destruction

**Cyber Criminals**

**Goal:** Financial Gain
**Activities:** Intentional, criminal

**Ability Characteristics:**
Vary widely
Disruptive use of ransomware
Some evade detection, using stealthy infrastructure

**Insiders**

**Goals:** Vary
**Actions:** Accidental, Intentional Abuse, Espionage, Financial

**Ability Characteristics:**
Can vary in abilities and intention
Known for trusted level of access
Inherent threat posed by these accesses

**Criminal Hackers**

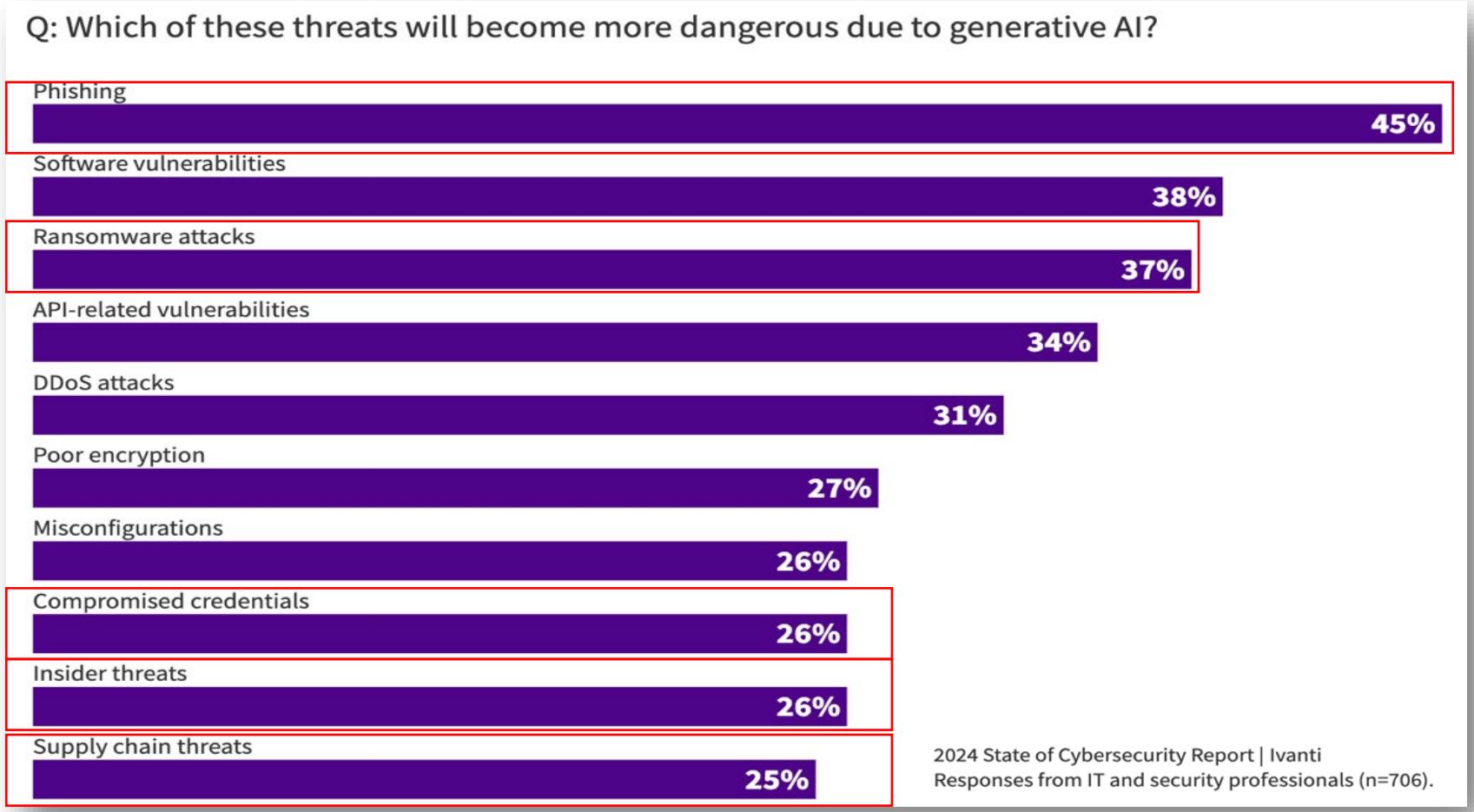
**Goals:** Draw attention to cause
**Actions:** Deliberate targets and times

**Ability Characteristics:**
Often, but not always limited
Enabled by 'hacking as a service'
PII disclosure
Attention-grabbing actions

**Secondary effects:** Damage to credibility and public trust

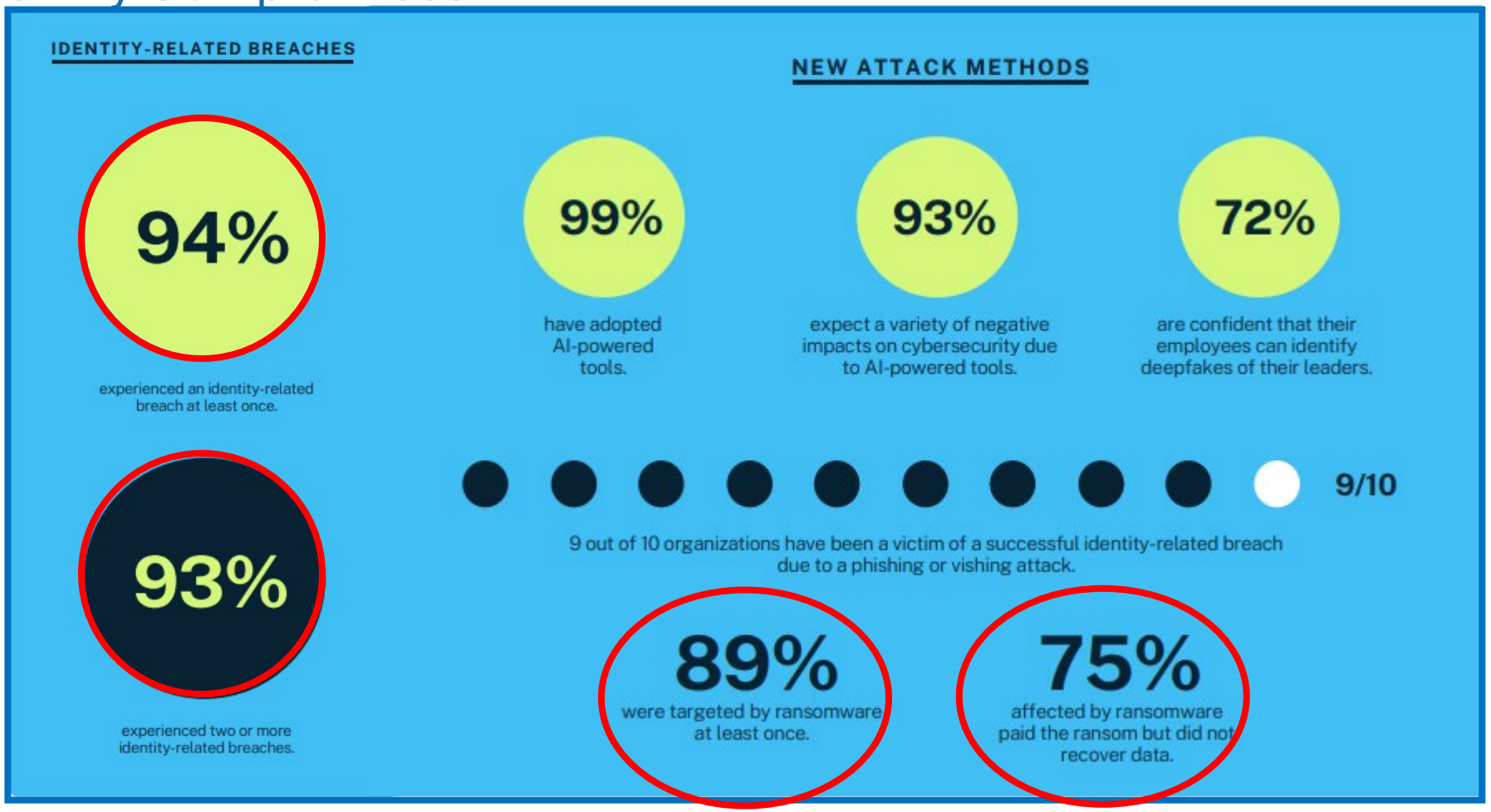
# Global Cybersecurity Industry Overview

- AI-powered threats loom large for security professionals



# Global Cybersecurity Industry Overview

## Identity Compromises




*Source: CyberArk, 2024 Identity Security & Threat Landscape Report*

# Global Cybersecurity Industry Overview

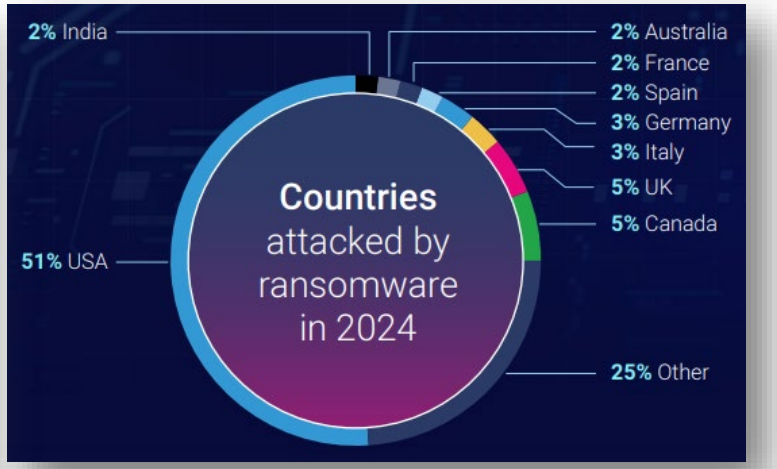
- Ransomware attacks in 2024

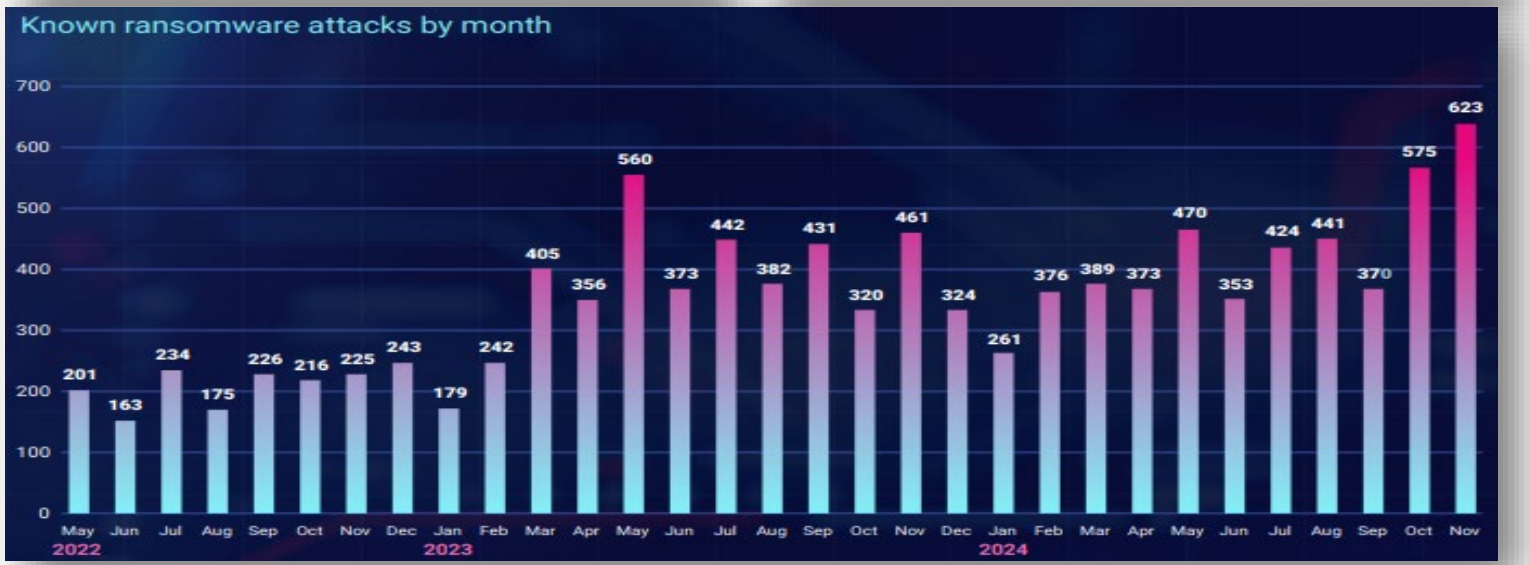


*Source: Threat down 2025 state of malware report*

# Global Cybersecurity Industry Overview

- Ransomware attacks in 2024


*Source: Threat down 2025 state of malware report*

# CSS Cyber Services Areas

# EIS – Cyber Security Services (CSS)

*Ben Gherezgiher*
*Chief Information Security Officer*

Cyber Security Services brings together a full suite of enterprise cybersecurity services – governance, infrastructure, cloud security, operations, architecture - under a single, accountable enterprise focused program. This allows for end-to-end direction setting and execution for enterprise security. CSS personnel work collaboratively with Data Center Services domain teams to deliver secure solutions to our customers.

- Cybersecurity Administration
- Security Architecture
- Security Governance, Risk and Compliance
- Network Security Services (Enterprise)
- Security Assessment
- Security Operations Center (SOC)

# CSS – Enterprise Security Operations Center (ESOC)





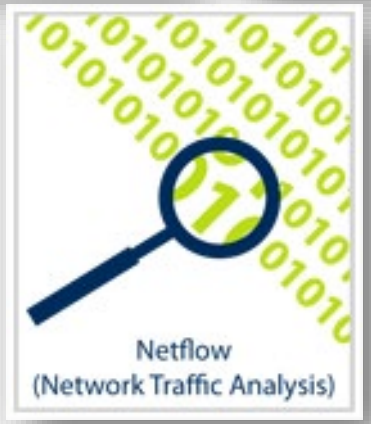



# CSS – Network Security Services (Net-Sec)











ENTERPRISE information services

# Cyber Security Services

## Cybersecurity Governance


## Cybersecurity Assessment


## Cyber Architecture

# CSS Statewide Cyber Standards

# Adoption of NIST Framework 2.0


# Cyber Security Services Operational Goals

- **Govern:** Cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify:** Implement cybersecurity risk management measures and risk management processes to reduce cybersecurity risks across the enterprise.
- **Protect:** Develop and implement enterprise safeguards to reduce risk and increase awareness and resiliency.
- **Detect:** Develop tools and processes to accelerate notification of cybersecurity threats; defeat threat actors before they have impact on state information assets.
- **Respond:** Consistently respond to anomalies and suspected events.
- **Recover:** Develop and implement an incident triage, response, and recovery process to contain and eliminate cybersecurity threats.

# Cloud M365 Security Framework

## Microsoft 365 Cyber Risk Framework

**Business Value**

**Business Objectives**

| Growth/ Innovation | Operational Efficiency | Security & Risk Management | Monitoring | Regulatory Compliance |
|---|---|---|---|---|

**Microsoft 365 Cyber Risk Governance**

**Governance**

| | | | | |
|---|---|---|---|---|
| Governance & Operating Model | Strategy & Roadmap | Information Governance | Policy, Standards & Procedures | Risk & Compliance Management |
| Cloud Security Guardrails | Secure Baseline Configuration | Insider Risk Management | eDiscovery & Legal Hold | Security Training & Awareness |

**M365 Cyber Risk Domains**

**Identity & Access Protection**

- Azure AD Identity Syncing
- Conditional Access
- Privileged Access Management (PAM) & Just-in-Time (JIT)
- 3rd Party Applications & Connections
- RBAC & User Lifecycle
- Identity Protection
- Access Reviews

**Data & Email Protection**

- Data Protection Policy & Controls
- Data Classification
- Purview Data Loss Prevention (DLP)
- Data Encryption
- Data Discovery
- Defender for Cloud Apps (CASB)
- Data Governance
- Email Security and Malware Blocking

**Endpoint Protection**

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Workstation Management (Windows 10 / 11)
- Endpoint Security & Encryption
- Windows Autopilot
- Endpoint detection and Response (EDR)

**Logging & Monitoring**

- Audit Logging
- SIEM Integration
- Cloud Security Posture Management (CSPM)
- Microsoft 365 Defender
- Microsoft Defender for Identity
- Endpoint Device Reporting
- Alert Policies

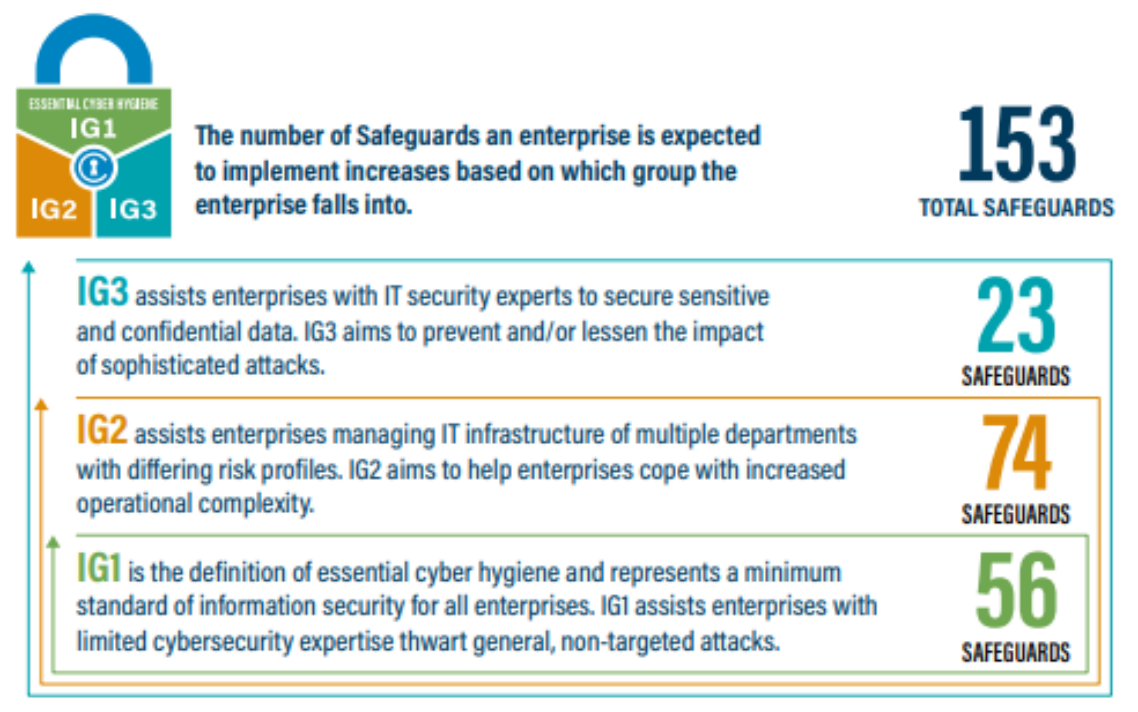
| Know Your Assets | Know Your Data | Know Your Customers | Know Your Employees | Know Your Third Parties | Know Your Attackers | Know Your Services/Processes |
|---|---|---|---|---|---|---|

# NIST 800-53 Security Control Families, Release 5

| Code | Description |
|---|---|
| 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 |

| Code | Description |
|---|---|
| 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 |

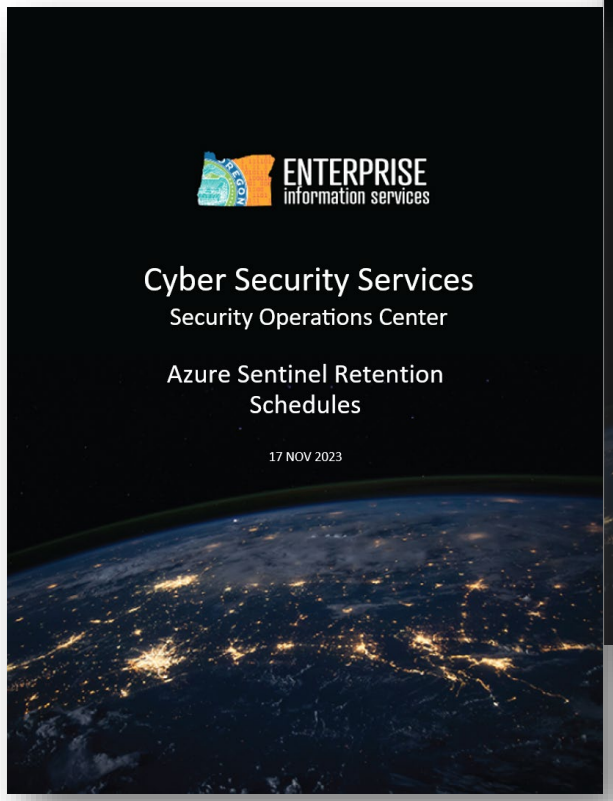
# Value of Cyber Assessments



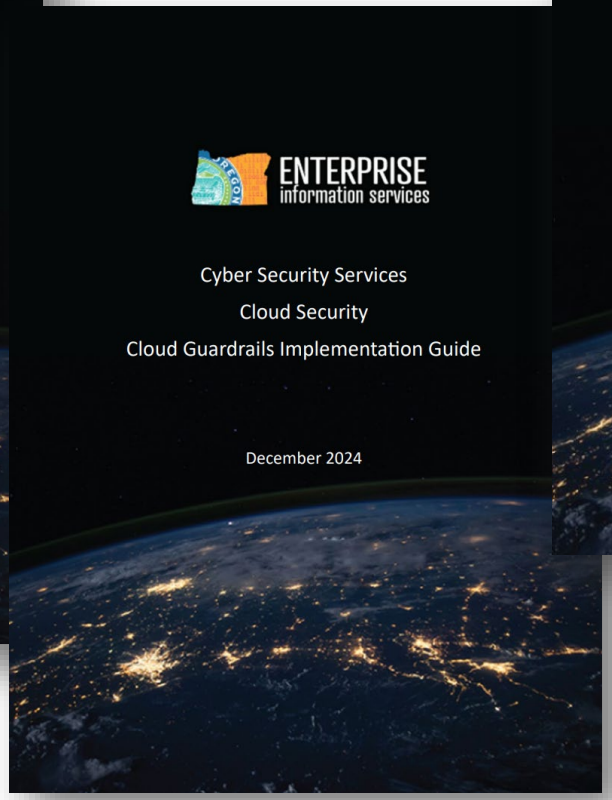

| Top 5 Attacks | IG1 CIS Safeguards<br>IG1 can defend against XX% of ATT&CK (Sub-)Techniques | All CIS Safeguards<br>CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques |
|---|---|---|
| Malware | 77% | 94% |
| Ransomware | 78% | 92% |
| Web Application Hacking | 86% | 98% |
| Insider Privilege and Misuse | 86% | 90% |
| Targeted Intrusions | 83% | 95% |

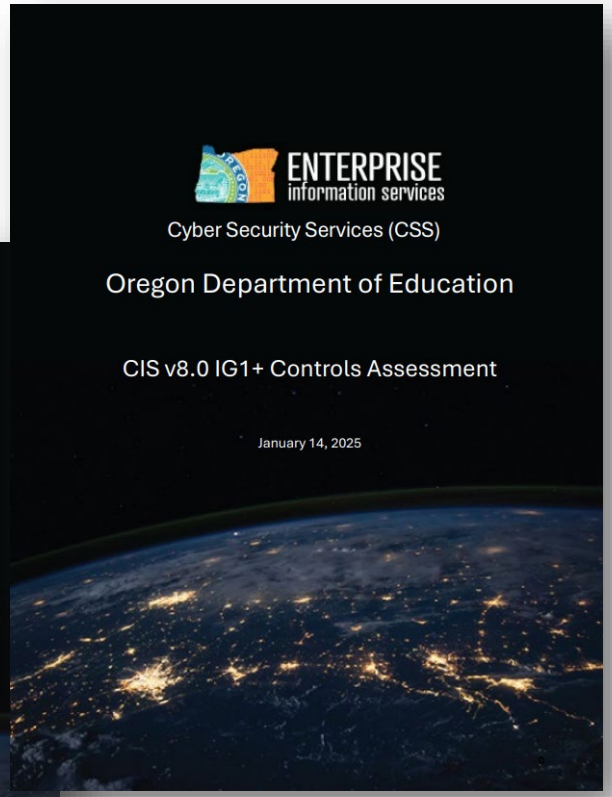
Complete implementation CIS V8.0 IG1 controls shows an average of 82% defense capability achievement against the top 5 attacks listed above.

# Institutional Documentation







# Cybersecurity Plans and Guides

# CSS Cyber Assessments

# Cybersecurity Assessments 2023-2025

- Assessments Completed

**July - December 2023**

- 31 CIS control assessments
- 1 web app assessment
- 3 CISA RVAs

**January - December 2024**

- 14 CIS control assessments
- 2 web app assessments
- 4 CISA RVAs

- Assessment Activity Targets for January – June 2025:
  - 25 CIS control assessments
  - 4 web app assessments
  - 4 CISA RVAs

CIS – Center for Internet Security
CISA – Cybersecurity and Infrastructure Security Agency
RVA – Risk and Vulnerability Assessment

ENTERPRISE information services

# Cybersecurity Assessments 2023-2025

## Ad Hoc Services

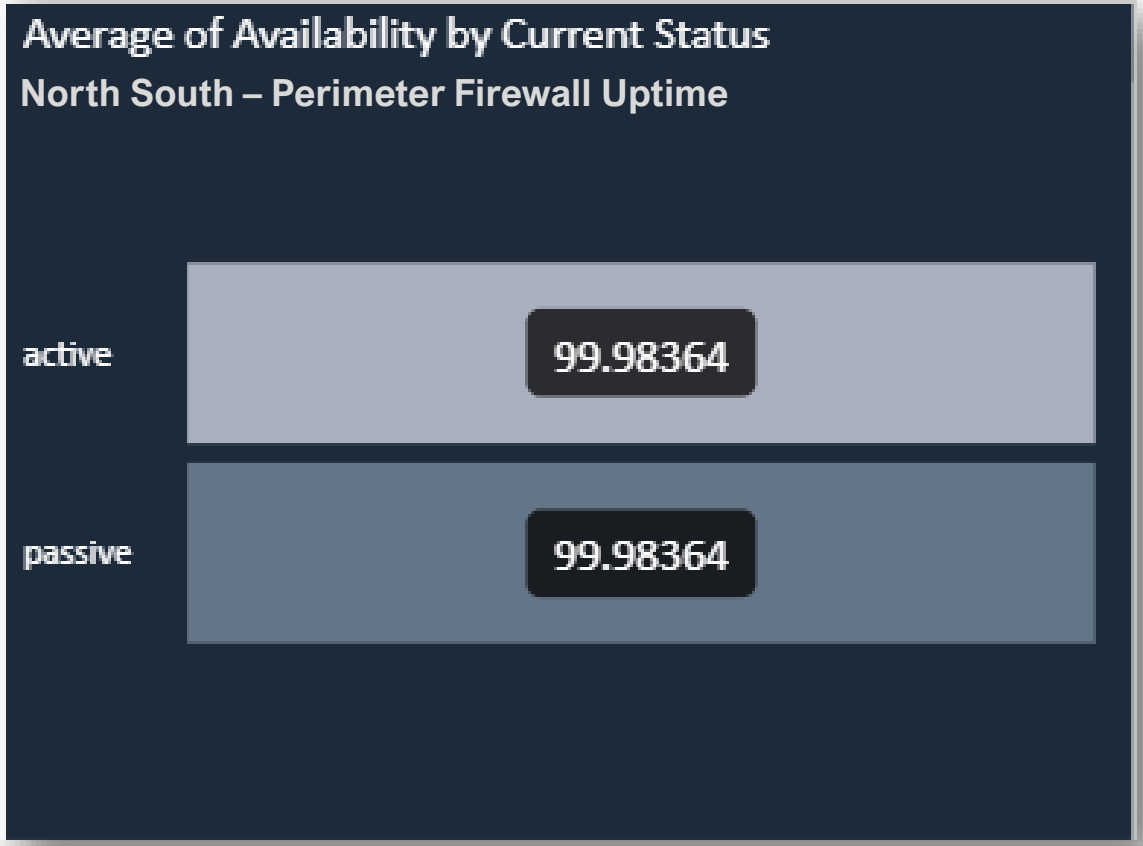
- AD Attack Path Analysis (BloodHound)
- Threat Modeling
- Vulnerability Analysis
- Open-Source Intelligence (OSINT) Analysis
- Known Exploited Vulnerability Enumeration
- Adversary Emulation
- Penetration Testing
- Cloud Security Analysis

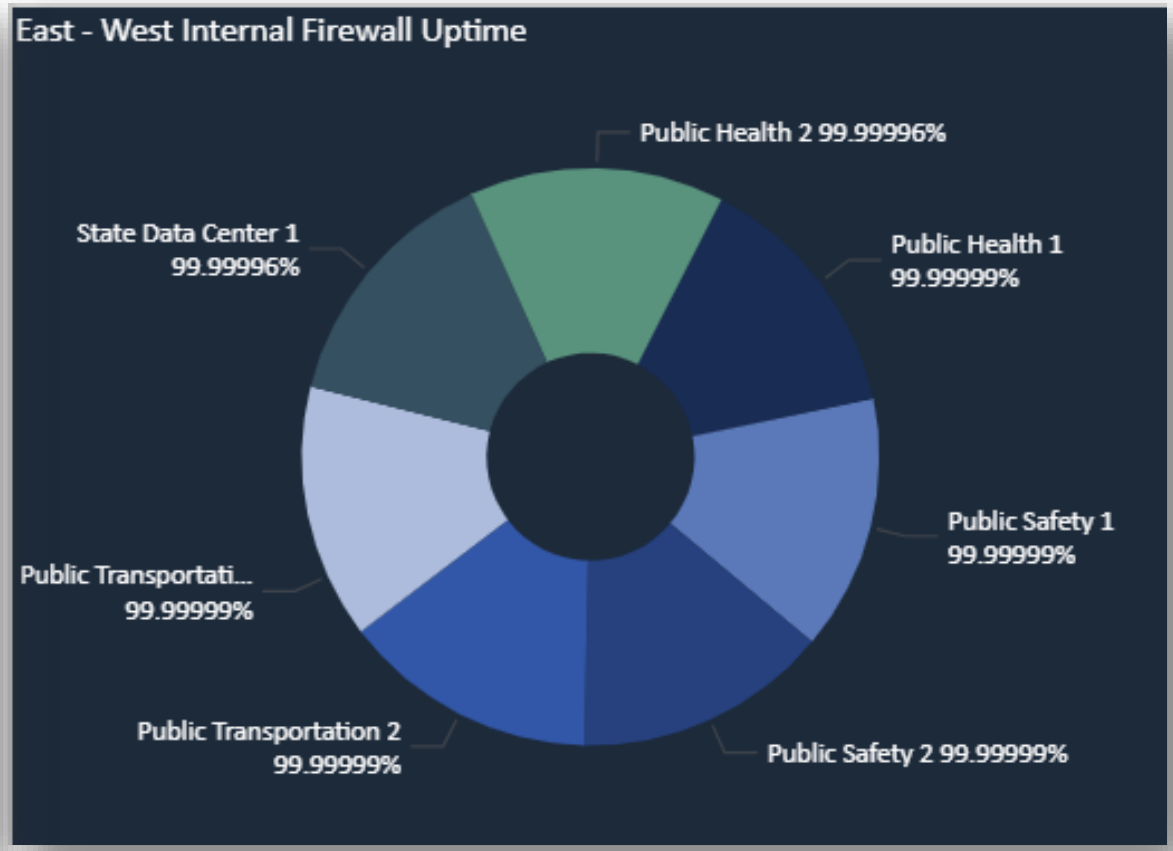
ENTERPRISE information services

Cyber Security Services

# CSS High Level Metrics

# Network Security Infrastructure Uptime



# CSS Projects and Initiatives

# Cyber Security Services

## Projects – In Flight

- Microsoft 365 Security Enhancements
- Network and Security Modernization Program
- Enterprise Mobile Security

## Initiatives – In Flight

- Integrated Risk Management Portal
- Enterprise Identity and Access Management Roadmap
- Modernize Network Threat Detection and Response (NDR)
- 24/7 managed service implementation for the ESOC

# Proactive Cyber Threat Monitoring Capability

# CSS Cyber Awareness and Partnerships

# Partnership Building Across Oregon


# Cybersecurity Awareness Campaign

ENTERPRISE information services
CYBER SECURITY SERVICES

RANSOMWARE AWARENESS CAMPAIGN

July 2023 | Volume 1

IDENTIFY, PROTECT, DETECT, RESPOND AND RECOVER

## What is Ransomware? & How Does it Happen?

Ransomware is a type of malicious software that encrypts the data on a victim's device or network and demands a ransom for its decryption. The ransom is usually paid in cryptocurrency or other untraceable forms of payment.

If the ransom is not paid within a specified time, the data may be permanently deleted or exposed to the public. Ransomware attacks can cause significant damage to individuals, businesses, and organizations by disrupting their operations, compromising their privacy and security, and extorting large sums of money.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's been infected with malware. Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More menacing versions can encrypt files and folders on local drives, attached drives, and even networked computers.

**GOAL: The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.**

### Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm
» October 13, 2023 9am – 10am

SOME COMMON RANSOMWARE VECTORS OF ATTACK ARE:

- Phishing emails with malicious attachments or links
- Exploiting unpatched vulnerabilities in software or systems
- Remote desktop protocol (RDP) compromise or brute force
- Drive-by downloads from compromised websites
- Network propagation through shared drives or devices

For more information scan the QR code or visit our website ransomwareinfo.oregon.gov

ENSURING ACCESSIBLE, RELIABLE AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

ENTERPRISE information services
CYBER SECURITY SERVICES

RANSOMWARE AWARENESS CAMPAIGN

August 2023 | Volume 2

IDENTIFY

## Identify

Identify, the first of five core functions within what is called the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), is widely adopted by organizations as a flexible and adaptable tool for improving their cybersecurity posture. It also provides a structured approach to assessing and managing cybersecurity risks, regardless of an organization's size, industry, or sector.

**CSF consists of five core functions: Identify, Protect, Detect, Respond and Recover.** By using the CSF, an organization can assess its current cybersecurity posture, identify gaps, and prioritize actions to improve its resilience against ransomware and other cyber threats. Organizations can also use it to align their cybersecurity efforts with their business goals, prioritize investments, and communicate their cybersecurity practices to stakeholders effectively.


GOAL: The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

### Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm
» October 13, 2023 9am – 10am

IDENTIFY IS ESSENTIAL FOR:

- Understanding your computing environment
- Assessing risks to the protection of customer data
- Determining the resiliency of services that rely on technology
- Creating disaster recovery or business continuity plans
- Preparedness when responding to a cyber security incident

For more information scan the QR code or visit our website ransomwareinfo.oregon.gov

ENSURING ACCESSIBLE, RELIABLE AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

ENTERPRISE information services
CYBER SECURITY SERVICES

RANSOMWARE AWARENESS CAMPAIGN

August 2023 | Volume 3

PROTECT

## Protect

Protect is the second of five core functions within the Cybersecurity Framework (CSF). The function of protect is to limit or contain the impact of ransomware events. There are three categories within protect that we will cover.

**Identity Management & Access Control** – The purpose of Identity Management & Access Control is to limit who has access to information/systems and verify they are who they say they are. These include:

- Ensuring user accounts with administrator-level privileges are never used to browse the internet or access email. Employees should be directed to use a regular computer account for daily work.
- Ensuring unused or stale computer accounts are regularly reviewed and disabled or deleted.
- Requiring the use of long complex passwords/ passphrases with a regular password reset interval.
- Utilizing Multi-Factor Authentication (MFA) on cloud-based accounts, when possible.

**Awareness & Training** – Because most ransomware events start by exploiting an organization's users, security awareness training can be highly effective in mitigating potential ransomware events. These include:

- Phishing awareness training – Teach employees how to recognize suspicious emails and report them.
- Social engineering training – Train employees how to recognize attacks that try to trick them into sharing sensitive information by using manipulation, imperson-ation and persuasion.

GOAL: The goal of this campaign is to provide business leaders, IT teams, and stakeholders shareable and actionable information to protect, detect, respond, and recover in the event of a ransomware attack. Over the course of the next few months, the State of Oregon Cyber Security Services team will be sending out additional awareness fliers to share and help educate as many organizations and people as possible. A webinar will be conducted at the end of the campaign, to provide a discussion and answer session for interested parties.

### Cyber Security Services Webinar - Save the Date!

» October 11, 2023 1pm – 2pm
» October 13, 2023 9am – 10am

PROTECT IS ESSENTIAL FOR:

- Understanding the need for different technologies to help mitigate ransomware events
- Stopping ransomware from reaching your users
- Blocking harmful or malicious content before they reach your systems
- Limiting the effect and impact of ransomware events

For more information scan the QR code or visit our website ransomwareinfo.oregon.gov

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

# Water and Wastewater Sector Cyber Guidance

CYBER SECURITY SERVICES

## Water and Wastewater Sector Cyber Guidance

Oregon's water and wastewater systems (herein referred to as "water systems") are part of the critical infrastructure that provides vital services to its citizens every day, however these same critical lifelines are also a target of cyber threats on a regular basis.

Water systems are targeted by malicious cyber groups and nation states alike, including those associated with the Iranian Revolutionary Guard Corps (IRGC) and the People's Republic of China (PRC) such as CyberAv3ngers[1] and Volt Typhoon[2], respectively. These malicious groups have targeted both Information Technology (IT) and Operational Technology (OT) systems, looking for any vulnerability that can be exploited to either make an immediate impact, or develop a foothold in the network for a targeted opportunity. Where any water system incident can result in a severe and damaging impact to the organization and the entire community, a continued dedication to cybersecurity best practices and planning are required and can establish an immediate improvement.

Cybersecurity best practices can scale from simple to in-depth, and some of the easiest changes can immediately defend against vulnerabilities recently exploited in attacks to water systems. Some best practices, resources, and contact information from both Enterprise Information Services (EIS) and our federal partners have been included.

1 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a
2 https://www.cisa.gov/news-events/news/us-and-international-partners-publish-cybersecurity-advisory-peoples-republic-china-state-sponsored

### Best Practices

| Immediate & short-term | Medium- to long- |
|---|---|
| Change default passwords immediately | Review/update pla policies with best p |
| Update software to address known vulnerabilities | Exercise plans to pr respond, and recov |
| Conduct cybersecurity awareness training | Inventory assets ar backup systems |

### Initial Recommendations

Initial recommendations include the below and in other actions to help protect vital services provide Oregon:

- Communicate with your State & Federal cybe
- Reduce exposure to public-facing internet
- Conduct regular cybersecurity assessments
- Change default passwords immediately
- Conduct an inventory of OT/IT assets
- Develop and exercise cybersecurity incident r and recovery plans
- Backup OT/IT systems, immutable if possible
- Reduce exposure to vulnerabilities
- Conduct cybersecurity awareness training

For more information scan the QR code or visit our website security.oregon.gov

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGO

### Resources

**Cybersecurity & Infrastructure Security Agency (CISA)**

- Top Cyber Actions for Securing Water Systems | CISA
- Water and Wastewater Cybersecurity | CISA
- Critical Infrastructure Sectors page, that includes sector information and resources to include a sector-specific plan, working groups, and additional publications.
- Low- and no-cost services, including exercises, assessments, training, and more

**Environmental Protection Agency (EPA)**

- Drinking Water and Wastewater Resilience page
- Cybersecurity for the Water sector page which includes cybersecurity assessments, planning, training, response, and funding resources and information.
- Cybersecurity Technical Assistance Program that will support organizations in conducting an asset inventory.
- Cybersecurity Incident Action Checklist

**Oregon EIS Cyber Security Services (CSS)**

- Statewide guidance, policies, standards, and mo be found at our website https://security.oregon.

**Additional Resources**

- Multi-State Information Sharing and Analysis Cer (MS-ISAC)
- Water Information Sharing and Analysis Center ( ISAC) is the only all-threats security information for the water and wastewater sector

### Incident contact Information

**CISA**
report@cisa.gov | 888-282-0870 | Report Site

**EIS Security Operations Center (SOC)**
Eso.soc@das.oregon.gov | 503-378-5930 | CSS Site

For more information scan the QR code or visit our website security.oregon.gov

ENSURING ACCESSIBLE, RELIABLE, AND SECURE STATE TECHNOLOGY SYSTEMS THAT SERVE OREGONIANS.

## Water and Wastewater Systems Cybersecurity Assessment Form

State of Oregon

June - December 2024

TLP AMBER+STRICT

This document once completed is set to TLP AMBER+STRICT, DO NOT send or transmit it without appropriate security. If you have questions about how to share this document, please contact CISA or the state cyber team for instructions.

*DISCLOSURE RESTRICTION: This document is marked TLP:AMBER + STRICT. Disclosure is limited. Sources may use TLP:AMBER + STRICT when information carries foreseeable risk of misuse, in accordance with applicable rules and procedures for restricted use. TLP:AMBER + STRICT, information may be distributed within participants organization only. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/*

## Water Sector Cyber Security Action Plan

June 18, 2024

Enterprise Information Services – Cyber Security Services

TLP: Amber – For Official Use Only (FOUO)

ENTERPRISE information services

# Thank you

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