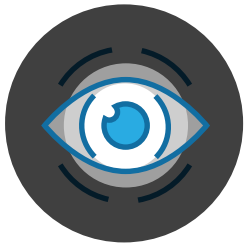# ENTERPRISE
information services
CYBER SECURITY SERVICES

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.

Protect

Detect

Respond

Identify

Cybersecurity Framework

Recover

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.

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

STATE OF OREGON
THE UNION
1859

Identify is especially important for ransomware defense, as it helps an organization to understand its assets, systems, data, and capabilities, as well as the potential risks and vulnerabilities that could compromise them. Some of the categories and subcategories under Identify are:

- **Asset Management:** The organization identifies and manages the physical and logical assets within its systems and networks, such as devices, software, data and users.

- **Business Environment:** The organization understands its role and mission in relation to its stakeholders, customers, partners and suppliers, as well as the legal, regulatory and contractual obligations that affect its cybersecurity.

- **Governance:** The organization establishes and implements policies, procedures and processes to manage and monitor its cybersecurity activities and performance.

- **Risk Assessment:** The organization identifies and analyzes the likelihood and impact of various cyber events on its assets, systems, data and capabilities.

- **Risk Management Strategy:** The organization develops and implements a plan to address the identified risks and mitigate their potential consequences.

By applying these categories and subcategories to its own context, an organization can create a comprehensive picture of its cybersecurity environment and identify the areas that need improvement or protection. This can help to prevent or reduce the damage caused by ransomware attacks, as well as to facilitate the detection, response, and recovery processes.

QUESTIONS TO DISCUSS WITH YOUR BUSINESS LEADERS:

» What are our most important organizational assets, business functions, and services we provide?

Additional Resources:

National Institute of Standards and Technology (NIST)
csrc.nist.gov

Cybersecurity & Infrastructure Security Agency (CISA)
cisa.gov/stopransomware
888-282-0870 | www.cisa.gov

FBI Field Office - Cyber Task Forces
fbi.gov/contact-us/field
Portland Office 503-224-4181
Ransomware Safety Resource

Multi-State Information Sharing and Analysis Center®
(MS-ISAC®) 866-787-4722

Oregon Cybersecurity State Incident Response Team
503-378-5930 | eso.soc@das.oregon.gov

Oregon Emergency Response System
(OERS) 1-800-452-0311

Statewide Interoperability Team
503-373-7251 | swic.or@das.oregon.gov

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

ENTERPRISE
information services

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