ENTERPRISE
information services

CYBER SECURITY SERVICES

RANSOMWARE AWARENESS CAMPAIGN

September 2023 | Volume 5

RESPOND

Respond

Respond is the fourth of five functions within the Cybersecurity Framework (CSF). Responding to a ransomware attack is a critical and time-sensitive process. It requires a well-defined incident response plan and a coordinated effort among various teams within your organization. Here are some items to consider, in the event of a ransomware attack:

Responding

- **Isolate the Affected Systems:** Immediately disconnect or isolate the infected systems from the network to prevent the ransomware from spreading further. This can involve isolating affected devices physically or by disabling network connections.
- **Confirm the Attack:** Ensure that the incident is indeed a ransomware attack by analyzing the ransom note, encrypted files, or any other indicators.
- **Activate the Incident Response Team:** Assemble your incident response team, including IT personnel, cybersecurity experts, legal counsel, and public relations specialists, if necessary.
- **Assess the Impact:** Determine the extent of the ransomware's impact, including the number of compromised systems and potential business disruptions. Determine what data may have been lost or compromised during the attack.
- **Identify the Ransomware Variant:** Identify the specific ransomware variant involved, as this information can help in assessing the severity and potential for decryption.

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 – 2:30pm
» October 13, 2023 9am – 10:30am

SOME EXAMPLES OF OUTCOMES WITHIN RESPOND:

» Mitigating the impact of a ransomware event
» Identification of the vector and source of the ransomware
» Successful data recovery without paying the ransom
» Enhanced security measures
» Good communication with stakeholders

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.

- **Activate your Incident Response Retainer:** If you've procured an incident response retainer with an outside company, consult with your incident response vendor. Incident response and forensics may be available to you.
- **Monitor for Resurgence:** Continuously monitor your network for any signs of the ransomware reactivating or other security threats. In many cases a previously offline system is missed and reinfects when reconnected to the network.

Communicating

- **Report the Incident:** Depending on your industry and location, you may be legally obligated to report the incident to data protection authorities and affected individuals.
- **Communicate Internally and Externally:** Maintain clear and regular communication with employees, customers, and partners about the incident's status and potential impact.
- **Notify Key Stakeholders:** Alert senior management, the IT team, legal counsel, and relevant stakeholders about the incident. Clear communication is crucial during an attack.
- **Engage Law Enforcement:** Contact local law enforcement or relevant authorities to report the incident. They may provide guidance and support during the investigation.
- **Legal and Regulatory Compliance:** Work closely with legal counsel to navigate any legal or regulatory requirements, such as data breach notification laws.
- **Don't Pay the Ransom:** While paying the ransom is tempting, it's generally discouraged. Paying the ransom doesn't guarantee that you'll get your data back, and it encourages cybercriminals to continue their activities.
- **Document the Incident:** Keep thorough records of all actions taken during all phases of the incident, as this documentation may be needed for legal or regulatory purposes.

A well-prepared and practiced incident response plan is crucial for effectively responding to a ransomware attack. It's essential to act swiftly, isolate the threat, and follow a systematic approach to minimize damage and data loss.

QUESTIONS FOR YOUR IT PERSONNEL:

- » Do we have an incident response plan?
- » Tabletop exercise?
- » Do we have everything we need to be ready to respond to a ransomware incident?

Additional Resources:

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

Cybersecurity & Infrastructure Security Agnecy (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.