

# CYBERSECURITY

Protecting Against  
Cyber Crime

# Risks to Public Agencies:

- ▶ **Public agencies continue to integrate tech into their day-to-day operations and nearly everything they do depends on their ability to create, maintain, and share large quantities of data.**
- ▶ **This data is increasingly at the core of fundamental services such as trash collection, building and zoning permitting, fleet management, public facility operations, utility maintenance, and even tree inventory.**
- ▶ **Public agencies are the top targets for cybercriminals, followed by education, healthcare, services, technology, manufacturing, and retail.**

# Current Cyberattack Stats:

- Every day in the United States, multiple local governments are hacked.
- Ransomware attacks are increasing. Ransomware complaints to the FBI increased by 82% from 2019 to 2021. Nearly 500 million attacks in 2021 and increased by over 60% in 2022.
- The average ransom paid by mid-sized organizations was \$211,260 in 2022.
- The average cost of resolving a ransomware attack was \$1.85 million. This cost includes downtime, people time, device cost, network cost, ransom paid, etc.
- The Oregon Department of Justice received 169 reports in 2021 of data breaches affecting at least 250 consumers.

# Examples:

Tillamook County, Linn County

St. Helens, Keizer, Portland

Centennial School District, PDX Public Schools, Treasure Valley CC

McMenamins, Yoshida Foods, Bob's Red Mill, Oregon Anesthesiology Group

# Cyber Crimes Include:

Illegal  
access

Illegal  
Interception

System  
Interference

Data  
Interference

Misuse of  
Devices

Fraud

Theft

# Avenues of Attack:



Any device that stores information or is connected to the internet can be a vulnerability



Any device connected to an agency's network



Remote access



Bluetooth



Open ports

## Examples:

- Smart devices
- Mobile phones
- Thermostats
- Vehicles
- Printers
- Medical equipment
- Industrial systems

# 5 Most Common Types of Cyberattacks:

Malware

Ransomware

Phishing

Data breach

Distributed Denial of Service (DDoS).

# What is Cyber Security?

- Cyber security standards enable organizations to **minimize** the number of successful cyber security attacks.
- Refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.
- Important for network, data and application security, as well as financial and operational security.



# Some Measures to Take:

- Cyber Insurance
- New technology and software updates
- Backup data
- Strict policies and training for employees

## Education and Awareness

Ask Good Questions

Know what your agency has in place (insurance, protocols, etc)

Build awareness

Enable multi-factor authentication (MFA)

Implement Internal Controls

## Risk Assessment

Don't be a Soft Target

Identify the most critical systems and what it will take to secure them.

## Backup and Patch

Keep software updated to the latest versions

Identify and back up critical data and store that information separately from the main network so it's harder for attackers to reach it

Patch software continually with the latest security updates.

## Monitor

Monitor system logs to look for suspicious activity

Tap Available Resources (ie. CIS, CISA, MS-ISAC, Shields Up, 3rd party)

## Practice and Prepare

Have a Security Incident Plan ensures everyone understands their role and has what they need to be able to perform their tasks - this includes IT, Fiscal, HR, Legal, and PR)

Run drills to work through responses to an attack

# CYBER SECURITY LANDSCAPE



# House Bill 2049 (2023):

**Cybersecurity Center of  
Excellence at Portland  
State University**

**Coordinate, fund or provide:**

**Cybersecurity education,  
awareness and training**

**Cybersecurity-related goods  
and services**

**Workforce Development**