SDIS

THIS IS NOT LEGAL ADVICE

Quick Reference Guide

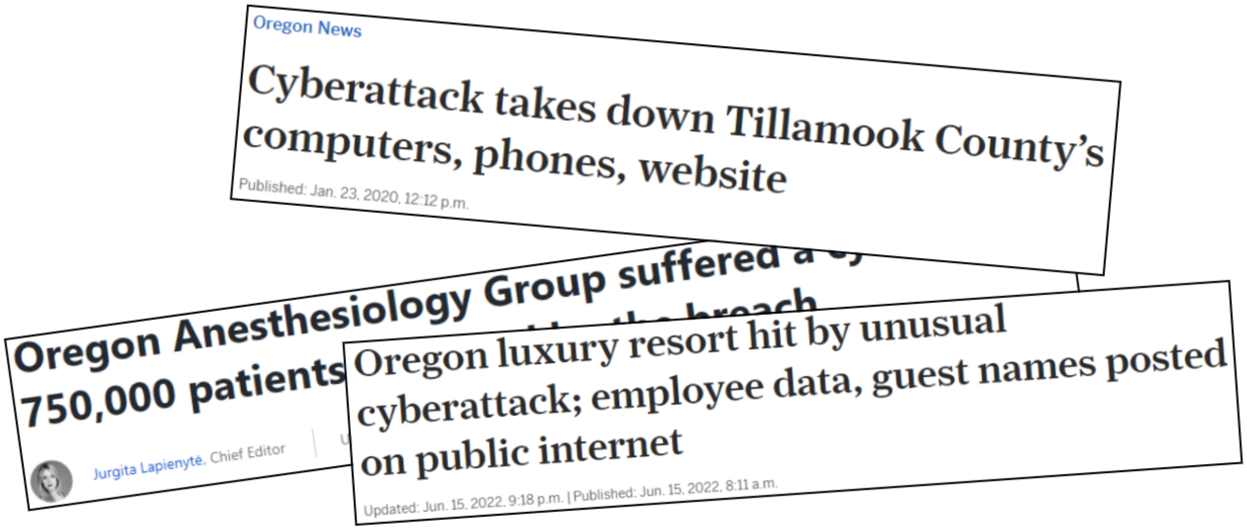
CYBERSECURITY

What is it?

Cybercrime is an ever-growing issue in today's business, and you need to be aware of it. It is not a matter of if it will happen, but when. While organizations scramble to perform thorough cybersecurity risk assessments, cybercriminals continue to exploit our vulnerabilities by aggressively outpacing our updates, patches, and firewalls. A 2021 study (Fox, 2022) identified an 11% increase in security breaches since 2018 and a 67% increase since 2014. In 2020, there were over 240,000 cybercrime victims from phishing alone (FBI, 2020) – that's without factoring in ransomware, identity theft, or personal data breaches! Additionally, in Oregon, cybercrime-related losses cost over $38 million in 2020 (FBI, 2020). Are your cyber defenses ready?

Is our organization really at risk of a cybersecurity attack?

Two of the biggest cybersecurity risks are ransomware and email fraud/phishing.



Oregon News

Cyberattack takes down Tillamook County's computers, phones, website

Published: Jan. 23, 2020, 12:12 p.m.

Oregon Anesthesiology Group suffered a cy

750,000 patients

the breach

Jurgita Lapienytė, Chief Editor

Oregon luxury resort hit by unusual cyberattack; employee data, guest names posted on public internet

Updated: Jun. 15, 2022, 9:18 p.m. | Published: Jun. 15, 2022, 8:11 a.m.

Consider asking yourself the following questions:

1. Do staff need an administrator password or privileged access to download apps and computer programs?
2. Are all organization-owned computers password protected?
3. If all organizational data was wiped or stolen today, are backups available?
4. Would your staff be able to recognize a phishing email if they saw one?
5. Are staff required to make strong passwords, and are these passwords set to expire?
6. If an employee's work laptop was lost or stolen, would organizational data be secure?

If you answered "no" to any of these questions, your organization is at an increased risk of a cybersecurity attack. Fortunately, there are many steps you can take to improve your cybersecurity practices.

How can we improve our organization's cybersecurity?

Here are several examples of actions you can take to secure your organization:

1. Create a secure foundation (examples: data back-up, password management, multi-factor authentication)
2. Limit administrative rights to only the IT department staff (examples: administration, district manager, IT staff)
3. Establish organizational policies (examples: acceptable use agreements)
4. Conduct cybersecurity awareness training (examples: cybersecurity training, email phishing exercises)
5. Secure your valuables (examples: accounting for deployed tech items, regular system updates, securing remote workers).
6. Plan for emergencies (examples: create an incident response plan, run tabletop exercises)
7. Proactive prevention (examples: 24/7 security detection, threat hunting)

The Cybersecurity and Infrastructure Security Agency (CISA) announced the establishment of the Ransomware Vulnerability Warning Pilot (RVWP) as authorized by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022. Through the RVWP, CISA will determine vulnerabilities commonly associated with known ransomware exploitation and warn critical infrastructure entities of those vulnerabilities, enabling mitigation before a ransomware incident occurs.

Organizations across all sectors and of all sizes are too frequently impacted by damaging ransomware incidents often perpetrated by cyber threat actors using known vulnerabilities. By urgently fixing these vulnerabilities, organizations can significantly reduce their likelihood of experience a ransomware event. However, most organizations may be unaware that a vulnerability used by ransomware threat actors is present on their network.

The RVWP will identify organizations with internet-accessible vulnerabilities commonly associated with known ransomware actors by using existing services, data sources, technologies, and authorities, including our free Cyber Hygiene Vulnerability Scanning service. CISA notifications will contain key information regarding the vulnerable system, such as the manufacturer and model of the device, the IP address in use, how CISA detected the vulnerability, and guidance on how the vulnerability should be mitigated.s

For more information on RVWP and other available resources for ransomware protection, detection, and response, all organizations are encouraged to visit StopRansomware.gov, a whole-of-government approach for ransomware resources and alerts.

Organizations interested with enrolling in CISA's Cyber Hygiene Vulnerability Scanning – contact vulnerability@cisa.dhs.gov

If you have any questions or concerns, please contact the Risk Management Department at 800-285-5461 or riskmanagement@sdao.com.

RESOURCES

Want more information? See our full-length Cybersecurity Guidebook from Eide Bailly (available in our Resource Library), provided to all members for FREE by SDAO.

Webpages

Cybersecurity & Infrastructure Security Agency (CISA)
4 Things You Can Do to Stay Cyber Safe (CISA)
CISA Multifactor Authentication
Cybersecurity Resources (PACE)
The Oregon Cyber Disruption Response and Recovery (OCDR) - Voluntary Resource Guide for Local Government
Information Sharing and Analysis Centers (ISACs)
Multi State-ISAC (MS-ISAC) – open to all State, Local, Tribal, and Territorial (SLTT) government organizations. Membership is free – register here.
CISA Services Catalogue

PDFs

Capacity Enhancement Guide for Organizations: Implementing Strong Authentication (CISA)
Implementing Phishing-Resistant MFA (CISA)
Multi-Factor Authentication Fact Sheet (CISA)

Videos & Webinars

Cyber.org YouTube Channel
Building & Funding a Cybersecurity Program (SDAO)
Cybersecurity Basics and Best Practices: Protecting Yourself from Common Cyber-Attacks and Threats (SDAO)
Cybersecurity: CIS Controls (SDAO)

Training

KnowB4 Cybersecurity Training
Vector Solutions/SafePersonnel (FREE to SDAO members! Contact ***riskmanagement@sdao.com*** for more information.)

National Guard – May be able to provide assessment work. (Contact ***riskmanagement@sdao.com*** for more information.)

Cybersecurity Self-Assessments

Nationwide Cybersecurity Review (NCSR)

Citations

Jacky Fox Managing Director - Accenture Security, Security, M. D.- A., Ryan LaSalle Senior Managing Director – Accenture Security, Senior Managing Director – Accenture Security, Paolo Dal Cin Lead – Accenture Security, & Security, L. – A. (2021, November 3). State of Cybersecurity Report 2021: 4th annual report. Accenture. Retrieved November 21, 2022, from https://www.accenture.com/us-en/insights/security/invest-cyber-resilience

Federal Bureau of Investigation (2020). Internet Crime Report 2020. www.ic3.gov. Retrieved December 19, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf