PACE

SAFETY • SERVICE • SAVINGS
A TRUST BUILT FOR STUDENTS

THIS IS NOT LEGAL ADVICE

QUICK REFERENCE GUIDE

CYBERSECURITY

Cybercrime is an ever-growing issue today, and you need to take steps to protect your organization. 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, cybercrime-related losses in Oregon cost over $38 million in 2020 (FBI, 2020). Are your cyberdefenses ready?

Is our organization really at risk of a cybersecurity attack?

Two of the biggest cybersecurity risks are ransomware and email fraud/phishing. Consider asking yourself the following questions:

1. Do staff members 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 were 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 may be at an increased risk of a cybersecurity attack. Fortunately, there are many steps you can take to improve your cybersecurity practices.

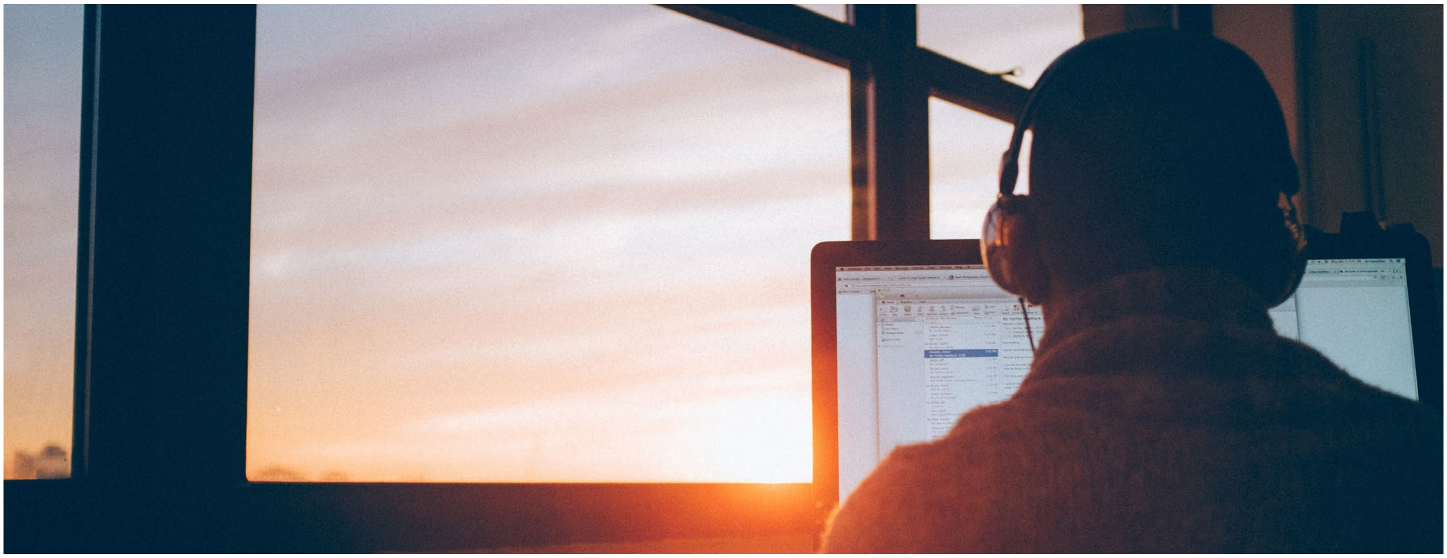
How can we improve our organization's cybersecurity?

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

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

PACE RISK MANAGEMENT

1-800-285-5461 • PACE.OSBA.ORG • RISKMANAGEMENT@SDAO.COM



WANT MORE INFORMATION?

Find cybersecurity resources below and contact riskmanagement@sdao.com with questions.

PACE Resources

- Cybersecurity resources
- Cybersecurity guidebook from Eide Bailly
- Cybersecurity framework webinar
- General cybersecurity awareness and best practices webinar
- Cybersecurity incident response plans

Additional Resources

- Cybersecurity & Infrastructure Security Agency
  - 4 things you can do to stay cybersafe
  - Multifactor authentication (MFA)
  - Capacity enhancement guide for organizations: implementing strong authentication (PDF)
  - Implementing phishing-resistant MFA (PDF)
  - MFA fact sheet (PDF)
- State of Oregon Cyber Disruption Response & Recovery Plan
- Nationwide Cybersecurity Review
- Information Sharing and Analysis Centers
- Multi State Information Sharing and Analysis Center
- Cyber.org (videos)
- KnowB4 Cybersecurity Training
- Vector Solutions|SafeColleges|SafeSchools (15 free courses for PACE members; contact **riskmanagement@sdao.com** for more information.)

If you have any additional questions or concerns regarding cybersecurity, please contact the risk management department at 800-285-5461 or riskmanagement@sdao.com.

rev. 02.2023

PACE RISK MANAGEMENT

1-800-285-5461 • PACE.OSBA.ORG • RISKMANAGEMENT@SDAO.COM

Home → Resources → Safety → Incident Reporting Materials