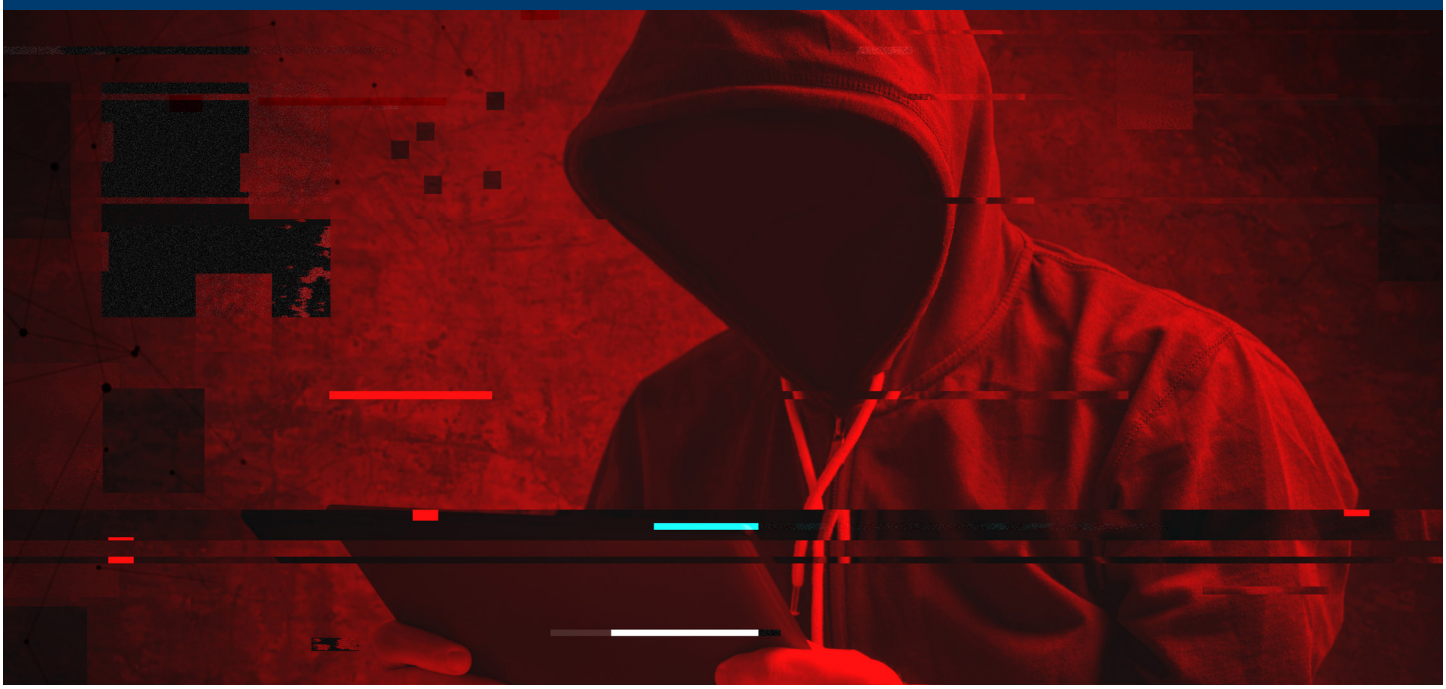
CIS Real-Time Risk



TIMELY NEWS AND TIPS TO HELP REDUCE RISK

January 2020

Cyberattacks Targeting Oregon's Cities and Counties

CIS is seeing a significant increase in the number of cyberattacks on cities and counties.

We are seeing three key areas of attack:

1. Entry into your system through email phishing to gain access to Personal Identifiable Information (PII) or Person Health Information (PHI);
2. Electronic Fund Transfer schemes where they trick the member in changing ETF for employee payroll or vendor accounts; and
3. Ransomware attacks initiated through emails. In the ransomware attacks the bad actor are asking for large ransoms ($100,000-$500,000) for the key to restore data.

CIS offers $50,000 of cyber liability coverage to all members with liability coverage. If you are interested in higher limits, contact your agent or Tena Purdy at tpurdy@cisoregon.org.

Continued on back

Real-Time Risk

Continued from previous page

It is critical employees are instructed not to open unfamiliar emails or go to unfamiliar websites. CIS recommends testing of employees to help teach them not to open unsafe emails.

Another critical safeguard is to have back up data on a daily basis in a safe location. Not only is the essential to maintain your coverage, but it is the only way to have the ability to restore your data.

CIS provides a cyber security sample policy. We request all members adopt and apply this policy. See the CIS website under Risk Management then Cyber Resources.

CIS contracts with cyber security consultants. If you have cyber security consulting needs, please contact Scott Moss and he will place you in touch with EideBailly.

CIS performed a cyber best practices assessment of members in 2018. These best practices are more important than ever. Please review these best practices with your IT professionals.

General Questions

- Do you have the means of identifying unauthorized hardware?
- Do you have the means of identifying unauthorized software installations on your network?

Protection Questions

- Do you employ industry-accepted configurations/standards for mobile devices, laptops, workstations, and other hardware and software?

eRiskHub® - Cybersecurity Resources

CIS members with liability coverage have access to eRiskHub® - a highly specialized web portal available to support privacy and network security needs of cities and counties.

Additional information about eRiskHub® is available on our website at cisoregon.org/cyber.

Continued on next page

Real-Time Risk

Continued from previous page

- Do you limit the number of users with administrative privileges?
- Do you require users to have a complex password?
- Do you utilize multi-factor authentication?
- Do you employ email attachment filtering practices (i.e. whitelisting and/or blacklisting)?
- Do you utilize filtering technologies to block incoming phishing and spam emails?
- Do you have technologies (i.e. web proxies/web filtering) in place that limit your users' access to dangerous or malicious sites?
- Do you have a process to properly back up critical information with a proven methodology for timely recovery of back up?
- Do you securely configure your network devices?
- Do you monitor the flow of data across the network?
- Do you employ encryption for your devices (where appropriate)?
- Do you segment your network based on the sensitivity of the data traversing it?
- Do you maintain appropriate wireless security, including the process and tools used to track, control, and prevent unauthorized use of networks?
- Do you have written on-boarding and off-boarding policies and procedures for employees and contractors?
- Do you have ongoing security awareness training?
- Do you perform periodic phishing exercises or social engineering tests?

Emerging Cyber Threats: Risk Mitigation Strategies

Join us on Thursday, Feb. 27 at the CIS Annual Conference where Sean B. Hoar of Lewis Brisbois Bisgaard & Smith, LLP, reviews emerging online threats including ransomware attacks, business email compromises, and social engineering — as well as the malicious evolution of data monetization. Sean will provide strategies to mitigate cyber liability risks and the stifling costs of ransom payments, fraudulent wire transfers, business interruption, regulatory enforcement actions, and third-party litigation.

Register today at cisoregon.org/conference.

Continued on next page

Real-Time Risk

Continued from previous page

- Do you identify the specific knowledge, skills, and abilities needed to defend the organization?
- Do you or your vendors employ secure coding practices for your websites, apps, and other programs?
- Do you employ web application firewalls on web servers, if you host your own website?
- Do you have a third-party vendor perform periodic external penetration tests on your network?
- Do you require verbal or face-to-face confirmation of changes to ETF bank changes.

Detection Questions

- Do you monitor your logs (firewall, system, and web logs) for anomalies and security violations?
- Do you employ automated tools to monitor workstations, servers, and mobile devices with anti-malware and host-based firewalls, and are they kept up to date?
- Do you manage the ongoing use of ports, protocols, and services on networked devices in order to minimize vulnerabilities?

Response Questions

- Do you or an outside vendor perform periodic network and web application vulnerability assessments?
- Do you apply security patches to operating systems and applications on a regular basis?

Recover Questions

- Do you have an incident response plan for cyber security incidents?
- Do you have an Oregon Consumer Protection policy?

For additional information, attend the CIS Conference February 26-28 and a Cyber Security Webinar scheduled for April 9.

If you have any questions contact P/C Trust Director Scott Moss, smoss@cisoregon.org or 503-763-3840.