CIS Real-Time Risk

TIMELY NEWS AND TIPS TO HELP REDUCE RISK

June 2021

NEW CIS CYBERSECURITY GRANT, REFLARE PARTNERSHIP

By Lisa Masters, CIS Senior Risk Management Consultant

In 2017, CIS started working with the other CIS — the Center for Internet Security — in an effort to prevent the cyberattacks that were foreshadowed. The first step was to conduct a cybersecurity risk assessment. Following the assessments, we developed a sample cybersecurity policy that our members could easily implement. Having a cybersecurity policy in place is a requirement for coverage. We also intensified our focus on cybersecurity by providing more trainings and additional cybersecurity resources.

In the last five years, CIS has paid over $718,000 in cyber claims. Of the 39 claims filed, 14 of those went to litigation, while one claim alone was almost $145,000.

Costly cyber related claims could be avoided by following these best practices.

Cyber claims fall in three areas:

1. *Fraudulent Instruction*
2. *Data Breach*
3. *Ransomware*

Continued on next page

Real-Time Risk

Continued from previous page

PREVENTING A CYBER EVENT

Some of the tips to look for when you receive a questionable email are:

- Does the email address look correct? This will often inform you if an email is official.
- Are there spelling or grammatical errors?
- Is the salutation vague or irrelevant to your operations?
- Is the email asking for personal information? Most legitimate companies will not ask you to send personal information via email.
- If something seems off, contact the person supposedly sending the email via phone to confirm they in fact sent the email.
- Check for a signature line, which most legitimate senders will include.
- If the email seems to have a high degree of urgency, beware. Most likely the sender is trying to get you to make a split-second decision that might be the wrong one.
- Hover the mouse over the email and if something looks suspicious, do not click on it.
- Do not open attachments to an email unless you know the email is legitimate. Attachments or links are how most hackers install malware or ransomware on computers.
- If an email is questionable, delete it and immediately report it to your designated IT representative.

It is sometimes a good idea to have your IT manager or consultant set-up a header for emails that notifies the person receiving the email whether it came from inside the entity or outside the entity. If an email derives from outside the entity but says it is from a staff member, the receiver should be skeptical and call the sender to determine if the email is legitimate.

RESPONSE/RECOVERY AFTER A CYBER EVENT

According to Cyber Attorney Sean Hoar, there are some helpful guidelines for responding to a cyber incident. He recommends that you first create an incident response plan, mapped to the National Institute of Standards and Technology (US Department of Commerce) Special Publication 800-61 Rev. 2., Computer Security Incident Handling Guide.

It requires the following:

- Identification and contact information for internal responders, including leaders of each business unit — not just IT.
- Identification and contact information for external responders, and Master Services Agreements (MSA) should be in place with each of them.
- A check list of tasks to be completed at each phase of the incident

Continued on next page

Real-Time Risk

Continued from previous page

cycle to be assigned ownership and time frame for completion by the incident commander

- Identification of sensitive data sets and any legal regulations pertaining to them — such as PI, PHI, PCI, LEDS/CJIS, etc.
- Reference to and summary of applicable data breach notification statutes.
- Template holding statements for internal and external messaging.
- Template consumer and regulatory notification letters.
- Other information that might be relevant to the particular organization.

CIS does offer excess cyber coverage above the standard $50,000 offered through the liability coverage. Contact your agent to get a quote on excess cyber coverage if interested.

CIS CYBERSECURITY GRANT

We're currently reviewing training and phishing testing with a cybersecurity company called Reflare. This summer, we will receive feedback from select CIS staff and members who will go through the 13-training modules provided by Reflare.

Starting July 1, CIS will offer a matching cyber-security grant. The grant will cover 50% of the cost of the 13-training modules and phishing testing, with 50% being matched by the CIS member.

The 13-training modules can be accessed through the CIS Learning Center with a total cost of $21.06 per employee.

There are a limited number of spaces that have been purchased by CIS, so

PI – Personal Information

PHI – Personal Health Information

PCI – Payment Card Industry Data Security Standard

LEDS – Law Enforcement Data System

CJIS – Criminal Justice Information Services

Continued on next page

Real-Time Risk

Continued from previous page

grants will be awarded on a first-come, first-served basis so submit your application as soon as possible.

At CIS, we're committed to supporting the needs of our members by providing resources and training opportunities that reduce cybersecurity threats. Contact your CIS Risk Management Consultant if you have questions.

ADDITIONAL CYBERSECURITY RESOURCES

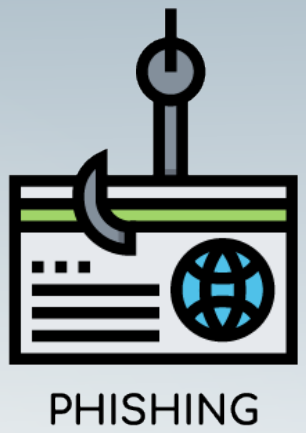
CIS has created a resource document with information from Portland State University Mark O. Hatfield Center for Cybersecurity on preventative methods.

Another is the January 2020 Real-Time Risk Article on "Cyberattacks Targeting Oregon's Cities and Counties," which leads you through the key areas of attack as well as questions to ask regarding your entity's preparedness for a cyber related attack or breach.

Also included in this article is an infographic that can help your staff identify a phishing email.

Lastly, CIS also has a sample IT continuity of operations plan in the CIS Risk Resource Library, which can help your entity with response planning for a cybersecurity breach or event. Visit our Risk Resource Library and select the Information Technology/Cybersecurity category for more cyber resources.

Detecting Suspicious & Malicious Emails



SENDER'S DISPLAY NAME

Does the email address look correct? This will often inform you if an email is truly from your manager, or not. You can spot a phishing email by finding inconsistencies in the sender's email address.

DON'T BELIEVE EVERYTHING YOU READ

If something seems off, contact the person supposedly sending the email via phone to confirm they in fact sent the email.

POORLY WRITTEN

Phishing emails often have grammatical errors, spelling mistakes, and are poorly written.

EMAIL SIGNATURES

Most legitimate external senders will include a full signature block at the bottom of their emails. This is not always the case but can help verify the legitimacy of an email.

GREETINGS AND SALUTATIONS

Is the salutation vague, odd, or irrelevant to your operations? This can be another indication of a phishing email.

BEWARE OF URGENT REQUESTS

Emails that require urgent action are often phishing emails. Cyber attackers will try to rush recipients into action before they can adequately study the email for authenticity. Read the email carefully before carrying out the action.

CAREFUL OPENING ATTACHMENTS

Do not open attachments to an email unless you know the email is legitimate. Attachments or links are how most hackers install malware or ransomware on computers.

CHECK LINKS BEFORE CLICKING

Hover the mouse over the email and if something looks suspicious, do not click on it.

DON'T PROVIDE PERSONAL INFO

Most legitimate companies will not ask you to send personal information via email.

WHEN IN DOUBT, THROW IT OUT

If an email is questionable, delete it and immediately report it to your designated IT representative.

CIS

citycounty insurance services
cisoregon.org