SHARING SINCE 2010
H-ISAC™
HEALTH - ISAC

Health-ISAC Monthly Newsletter –TLP White April 2021

# HEALTH-ISAC Hybrid Spring Summit

## "Secured in Paradise" May 18-20, 2021

Secured in Paradise
HEALTH-ISAC HYBRID SPRING SUMMIT
MAY 18-20, 2021 • NAPLES, FL

## View the Agenda

Thank you to everyone who submitted an abstract for consideration. We had quality submissions. Our Content Committee reviewed, rated and selected a great line up of sessions for the upcoming Spring Hybrid Summit.

View the full agenda here (https://cvent.me/eXbe3G)

### Virtual Platform

"Secured in Paradise" official dates are May 18-20 but why wait? The Virtual Platform will become available to registered attendees on May 3. Begin networking with other attendees. Schedule 1:1 meetings. Explore and watch as the platform grows and evolves leading up to the event kick-off. Get a head start on earning game points for fantastic prizes!

### Member Round Tables

Back by popular demand! Member Round Tables are small group discussions meant to be detailed and technical. Seats are limited. Registered members will have the opportunity to select which Round Tables they wish to attend when the virtual platform opens on May 3. These sessions fill up quickly.

## Ransomware Preparedness Tabletop Exercise (TTX)

Health-ISAC recently planned and conducted a ransomware preparedness virtual tabletop exercise with a member. The four-hour exercise consisted of 70+ participants engaged in both plenary and breakout group discussions focused on response to a ransomware attack. The desired outcomes of the exercise were in part to gain perspective on incident response, identify potential gaps, and learn from others to improve processes and procedures.

Quote 1
"Our team really got a lot of value from this tabletop exercise and we appreciated the relevance of the scenario to our general location and cyber threats. It would be helpful to do these somewhat regularly – altering the scenarios according to threat landscape. Not only does it give us a chance to build up playbooks for incident response by being guided through a potential attack, but it gives us the chance to discuss the topics with our peers within [our organization] in a way that is useful."

Quote 2
"This was a fantastic exercise that spawned a lot of "what if" and "do we have" and "what would you do" conversations amongst our team. We came away with several action items to help enhance our preparedness for Incident Response."

With the success of this pilot exercise, Health-ISAC will be offering a TTX as a service for members in the future. Interested members may contact the member engagement team to learn more or send an email to contact@h-isac.org using the subject line: 'TTX as a service.'

## Top Health Related April Cyber Events:

$4,000 COVID-19 Relief Checks Cloak Dridex Malware

Mimecast Reveals Source Code Theft in SolarWinds Hack

FBI: Over $4.2 Billion Officially Lost to Cybercrime in 2020

Report: 25% of UK Workers Let Their Children Use Their Work Device

Exchange Servers First Compromised by Chinese Hackers Hit with Ransomware

Hackers Hiding Supernova Malware in SolarWinds Orion Linked to China

Kremlin Calls NYT Report on Planned US Cyberstrikes on Russia Alarming

Virginia Consumer Data Protection Act Signed into Law

Microsoft Exchange Zero-Day Attacks: 30,000 Servers Hit Already, Says Report

FTC Joins 38 States in Takedown of Massive Charity Robocall Operation

H-ISAC is pleased to publish a monthly member newsletter. It is designed to bring events and other important ISAC information to your attention. If there is something you would like to see included please email: contact@h-isac.org

@H-ISAC @Health-ISAC

@HealthISAC

# HEALTH-ISAC THREAT OPERATIONS CENTER (TOC)

## Security Awareness Best Practices

By: Joshua Justice & Brad Regeski, Health-ISAC TOC

Security Awareness Training campaigns are effective resources for educating employees about common phishing tactics, techniques, and procedures. When developing training, be mindful to:

- Work with stakeholders to identify specific areas of concern to your organization.
- Develop a calendar of activities to address top concerns and risk factors through awareness training and phishing campaigns designed to equip your team with the knowledge needed to combat threats.
- Set reasonable, incremental goals. Be prepared to edit if initial approaches fail to produce positive results.
- Practice on-going assessments and training.
- Ensure security is a collective responsibility; ensure training is inclusive of all people, processes, and technologies.
- Deliver content that engages the audience and provides a foundation for a memorable training activity.
- Include a corrective landing page and/or instructional video at the conclusion of a simulated phishing attack.
- Avoid the use of any copyrighted material and/or logos as lures used in internal employee phishing campaigns. Reinforce that any third-party logo is for illustrative or instructional purposes only.
- Put metrics in place to assess the impact of your program and to demonstrate a return on investment.
- Provide opportunities for self-paced cybersecurity training for individuals seeking to develop knowledge on emerging threats.

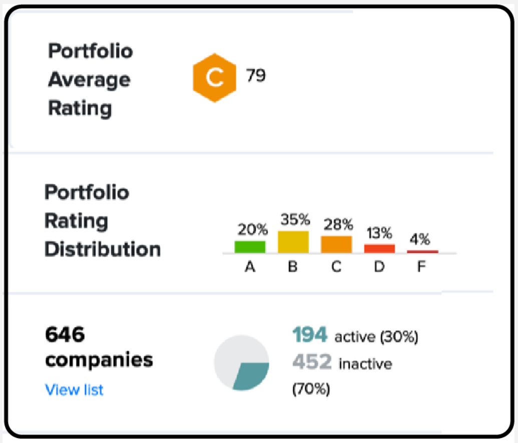
Successful security awareness training tools focus on the overall goal and mission. Developing behavioral change and increasing engagement will foster a culture of cybersecurity and transform your awareness training from an annual event into a sustainable corporate culture with demonstrable returns.

# SHARED SERVICES UPDATE

## WHAT'S IN A SCORE?

Health-ISAC's TOC and Membership Engagement Team have been working together by using security ratings to benchmark the cybersecurity programs of Health-ISAC members. By allowing us to see how organizations compare to others, and also how each health subsector within H-ISAC measures up, we hope to identify additional ways to help improve your cybersecurity hygiene.

*The average Health-ISAC member scores on March 25th:*



Portfolio Average Rating C 79

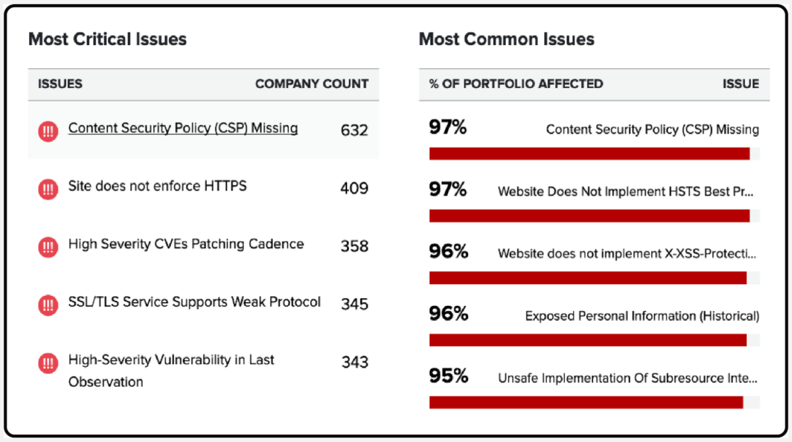
Portfolio Rating Distribution

646 companies

View list

194 active (30%)

452 inactive (70%)



**Most Critical Issues**

| ISSUES | COMPANY COUNT |
|---|---|
| Content Security Policy (CSP) Missing | 632 |
| Site does not enforce HTTPS | 409 |
| High Severity CVEs Patching Cadence | 358 |
| SSL/TLS Service Supports Weak Protocol | 345 |
| High-Severity Vulnerability in Last Observation | 343 |

**Most Common Issues**

| % OF PORTFOLIO AFFECTED | ISSUE |
|---|---|
| 97% | Content Security Policy (CSP) Missing |
| 97% | Website Does Not Implement HSTS Best Pr... |
| 96% | Website does not implement X-XSS-Protecti... |
| 96% | Exposed Personal Information (Historical) |
| 95% | Unsafe Implementation Of Subresource Inte... |

*SecurityScorecard provides Cyber Risk Ratings. With over 3 million companies scored, (20 Million by the end of 2021), SecurityScorecard lets companies continuously monitor and grade the External Cybersecurity Posture of ANY organization* (their scores have a statistically relevant correlation with breach risk)*. Customers leverage SecurityScorecard's solution to support a variety of use-cases that include, but are not limited to, Vendor Risk Management / Supply-Chain Risk Management, Enterprise Monitoring and Regulatory Compliance.*

**All Health-ISAC members** are entitled to a complimentary SecurityScorecard Enterprise license that enables you to monitor yourself and up to five third parties. To take advantage of the offer and see how you stack up to your peers, contact Health-ISAC Shared Services.

**Request access here https://h-isac.org/ssc-offer/**

# UPCOMING HEALTH-ISAC WEBINARS registration links https://h-isac.org/events/

**Protect Against DDoS and Ransomware Attacks as they Grow in Complexity by Netscout**

**04/06/2021 1:00 pm**

**The Criticality of Lateral Movement Detection by Attivo Networks**

**04/15/2021 1:00 pm**

**Managing and Activating Your Threat Intelligence by Cyware**

**04/20/2021 1:00 pm**