



IHS NEWSLETTER

Key Takeaways from the IHS Thought Leaders Conference

The recent IHS Thought Leaders Conference provided essential insights into enhancing crisis management. Here are the key takeaways:

Actionable Changes and Empowerment

Focus on improvements for frontline workers in critical infrastructure (CI) at local levels, empowering both executives and staff with the necessary knowledge for informed decision-making.

Addressing Emerging Threats

A coordinated risk management approach is vital, especially to counter foreign state actors. The healthcare sector faces significant cybersecurity threats, requiring proactive measures to strengthen resilience.

Collaboration and Partnerships

Collaboration between public and private sectors can effectively address challenges. Networking with researchers and industry leaders is crucial for enhancing training and resilience in critical sectors.

Resource Gaps

There's a need to better utilize available resources, particularly for small to medium-sized enterprises (SMEs). Supporting these businesses with knowledge in threat security is essential.

Implementation Challenges

Siloed approaches hinder effective integration of solutions, and interdependencies between infrastructure assets can lead to cascading risks, underscoring the need for coordinated action.

Crisis Communication

Develop clear intelligence and communication plans to manage misinformation and prepare for crises. Regular engagement in the healthcare sector is vital for addressing supply chain vulnerabilities.

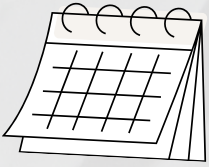
Research and Future Directions

Future research should focus on effective disaster communication strategies and creating a cross-sector crisis playbook. Resiliency training and collaboration will enhance overall preparedness.

Conclusion

The conference emphasized the importance of coordination, communication, and empowerment in crisis management. By implementing these strategies, organizations can improve resilience and effectively prepare for future challenges. Stay tuned for more insights on enhancing crisis readiness!

IHS also released a podcast discussing the event! Check it out at <https://ihsonline.org/>.



RESEARCH



[Online Research Link](#)



Who's in Charge of OT Security?

Joe Weiss

IT attacks are only part of what should make CSOs, CISOs and Risk Officers lose sleep. While IT cyberattacks often make the news, potentially more dangerous are Operational Technology (OT) cyberattacks and failures. Not only can the latter cause include explosions, destruction, injuries and death, but the way we protect OT can do so as well.

OT monitors and controls physical processes. Automating OT is more efficient and reliable than manual operations, keeps better records, doesn't need multiple rest periods every day, or have labor issues. When properly programmed, it doesn't make mistakes humans will, helps assist with maintenance and can warn of and mitigate danger. However, if hackers can bypass security and "take over" systems, the very processes OT protects can become extremely hazardous. This is

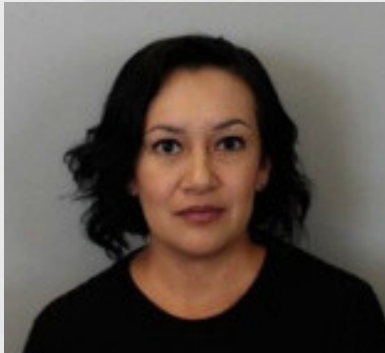


further compounded because some OT cyberattacks have been disguised as accidental OT issues. In more than one instance, a "failure of imagination has led security teams to misdiagnose cyberattacks as benign failures". One contributor to these "misdiagnosis" has been because the network protectors of OT do not fully understand the OT operation, communication, vulnerabilities, and how to safely protect OT. Regrettably, this lack of understanding can be dangerous. The goal of this paper is to help CSOs, CISOs, and Risk Managers be aware of OT cyber and safety issues so they can maximize IT and OT protection without endangering OT operation. CSO's need to work with engineering and operations to develop, implement, and maintain control system cyber programs as well as identify control system cyber incidents. Without understanding control system issues, cyber protections may not be sufficient to prevent cyberattacks that can damage hardware and cause injuries. On the other hand, inappropriate technologies or testing can, and have caused, the same impacts as hackers.

TEAM MEMBER HIGHLIGHT <<<

Cindy Martinez

Executive Coordinator



Mrs. Cindy Martinez is the current Executive Coordinator for the Institute For Homeland Security (IHS) at Sam Houston State University (SHSU). In this capacity, Cindy oversees multiple high level administrative projects while also managing scheduling and agendas for IHS leadership. As a former Administrative Associate at Prairie View A&M and after years in the field, Cindy brings to the team much needed knowledge in higher education policy and procedures. In addition to her full – time role at IHS, Cindy is currently pursuing her bachelor’s degree. Cindy has been recently awarded the IHS Cornerstone Award in recognition for her exceptional support and unwavering commitment to IHS. As a true pillar of our team, all of the IHS staff congratulate Cindy on this well-deserved honor!

>>> PODCAST <<<

DEFENDING CRITICAL INFRASTRUCTURE FROM POLITICAL POLARIZATION

Dr. Miyah Hutchens

Critical Infrastructure depends on collaboration and teamwork – not distraction and hostility dividing employees. Political polarization presents a threat to the public and private sector’s ability to develop and maintain critical infrastructure protections. In this episode, we’re joined by Dr. Miyah Hutchens, an associate professor and chair of the Department of Public Relations at the University of Florida, to explore workplace and personal strategies for reducing polarization and improving civility.

THE FUTURE OF AI DETECTION

Dr. Jason Davis

Generative AI programs can create a surge of bogus images, videos, and audio at a moment’s notice, often damaging trust, and credibility across critical infrastructure sectors. Our brains can’t keep up, but what about AI detection software? This week, we chat with Dr. Jason Davis of Syracuse University and Dr. Tony Yao of Sam Houston State University about how AI technology is outrunning our cognitive abilities and legal frameworks, and how emerging software may help close the gap.

EVENTS <<<

TRANSPORTATION ROUNDTABLE

- **Date:** November 19th, 2024
- **Time:** 8:30am - 1:00pm
- **Location:** SHSU Woodlands Center Room 109
- **Link:** [Register Here](#)
- Discuss vulnerabilities and risk mitigation for IHS research and education projects.

