Highlight

This month we explore Incident Response and how to effectively communicate after a cyber event. In our first article, **Phil Schenkenberg** and **Zenus Franklin** of Taft Law explain why organizations should adopt the word "incident" until legal counsel officially deems something a "breach." **Learn why** this allows for effective and accurate communication while avoiding legal pitfalls.

CyberBytes™

THE LOST ART OF INCIDENT RESPONSE COMMUNICATION
When cyber incidents occur, employing the critical skills, technology and resources to mitigate the threat is essential. But good communication before, during and after an incident is equally important, contends **Loren Dealy Mahler** (Dealy Mahler Strategies). **Read on** as Loren makes the case and offers actionable reminders to elevate your communication at each phase of an incident.

IMPROVING RESPONSE TIME WITH CYBER RANGES
Beyond the right skills, tools and resources, achieving a rapid response to a cyber incident requires practising with your response team ahead of time. One method is the use of hyper-realistic, flexible and highly-configurable cyber ranges. In his piece for Infosec Resources, **Patrick Mallory** explains **how these customizable environments can be leveraged** to reduce incident response time.

THINK TANK MEMBER HONORED
The United Nations Association – Minnesota Chapter (UNA-MN) recently **presented the Harold E. Stassen Award** to **Mark Ritchie** (Pres., Global Minnesota and Cyber Security Summit Think Tank Member). The award recognizes individuals who have spent "decades of their life promoting the mission and agenda of the United Nations, engaging in relentless advocacy work for international cooperation, and organizing and conducting numerous programs and events." Congratulations, Mark!

In Case You Missed It

- The Future of Cybersecurity: How to Prepare for a Crisis in 2020 and Beyond | SecurityIntelligence
- 3 Lessons From the Incident Response Tabletops | SecurityIntelligence
- CISA Tabletop Exercises Package | CISA
- How Organizations Can Ramp Up Their Cybersecurity Efforts Right Now |Harvard Business Review

Think Tank Perspective

Greg Ogdahl
Director, Defensive Cyberspace Operation, MoneyGram

Incident Response. A descriptive verb which is often used in a sentence containing words which no one likes to hear: breach, exfiltration, ransomware or cyberattack. By appending the word team, we get a noun. While we have plenty of nouns in cyber: firewall, IDS/IPS, VPN, encryption; it is in a team where we must focus our resources to enhance. A team is what is going to help reduce the recovery time, understand the incident, and ultimately reduce the attack vectors.

Sponsor Spotlight

www.cofense.com

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of over 25 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. **Visit Cofense®.**

Partner Spotlight

www.cisecurity.org

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. CIS is home to the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (MS-ISAC® and EI-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities and U.S. elections offices. Learn more at **www.cisecurity.org**.