Securing A Digital Southern California: Cyber Crime and SoCal's Private-Public Partnership – September 6, 2017

NACD Southern California held a lunch meeting on September 6, 2017 at The California Club in downtown Los Angeles titled "Securing A Digital Southern California: Cyber Crime and SoCal's Private-Public Partnership." In light of The National Cyber Forensics Training Alliance (NCFTA) recently opening its Los Angeles office, the discussion focused on Southern California's unique risks and local efforts to fight cybercrime.

The event was moderated by Bob Zukis, Board Director – NACD Southern California and featured panelists with backgrounds in the Secret Service, information security, and disruptive technologies: Matt LaVigna, Director of Operations and Interim President/CEO – National Cyber Forensics Training Alliance (NCFTA); Dr. Stan Stahl, Founder and CEO – Citadel Information Group and Jerry Sto. Thomas, CISO – Apria Healthcare Group, Inc. The panelists reflected on NCFTA's private-public efforts to identify, mitigate and neutralize cyber threats globally.

Key Takeaways:

1) Chief Information Security Officer

- Know when a CISO (Chief Information Security Officer) is needed. There are a lot of virtual CISOs, so consider your threshold and hire a virtual CISO if your company is not ready for a dedicated CISO. This is a critical step in helping your company prepare for a cyberattack. Remember that today, compliance is a false sense of security.

2) Board Leadership

- Boards have an opportunity to provide leadership on cyber security. Send the person accountable for IT to a conference – not the person who manages IT, the person who IT reports to. That's where leadership emerges to serve the company's security needs.

3) Organizations

- Join an organization. Find a place to learn more and participate in furthering the dialog such as servethevillage.com or LA Cyber Security Lab. There are many good places to learn more so don't start from scratch, follow the group.

4) Report Attacks

- Report it! If you get attacked, don't keep it to yourself. Remember, you are the victim – report cyberattacks to law enforcement.

5) Digital Diversity

- Don't be disillusioned. History shows us that over time the benefits of digital will be there. Through private public partnership, solutions will be created. Start with digital diversity - get the skills and expertise in the Boardroom.

Conclusion – Board Directors should feel empowered to lead cyber security measures and assign leadership if necessary. Knowledge is key and implementing preventative measures will be worthwhile in the long run.