NACD Texas TriCities Chapter | San Antonio

Cybersecurity Oversight
April 13, 2017

Program Moderator

- **Sharon O'Malley Burg:** Chief Executive Officer, O'Malley Burg Consulting; Board of Advisors, Infrastructure Resources, Inc.

Program Speakers

- **Maj. Gen. Suzanne "Zan" Vautrinot:** President, Kilovolt Consulting, Inc.; Major General, United States Air Force (Ret.); Director, Wells Fargo, Ecolab, Inc., Symantec Corporation, Parsons Corporation, and the Battelle Memorial Institute
- **Brian Kelly:** Chief Security Officer, Rackspace
- **Charlie Leonard:** Co-Founder and Chief Operating Officer, Cybernance

---

Program Summary:

In April, the Tri-Cities Chapter gathered in San Antonio for a discussion on cybersecurity. The talk covered current trends in the types of cyber-threats and the methods used to combat those threats. Throughout, the panelists focused the discussion on board oversight, offering insights on how to best equip directors to face this evolving, ever-present challenge.

Sharon Burg kicked off the program with a question: What's changed since the 1970s and '80s, vis-à-vis cyber-threats? Brian Kelly suggested that one of the biggest changes is that we now realize how hard cybersecurity can be. He suggested that the biggest weakness companies face is complexity. Unfortunately, he said, the public and private sectors have made big investments in cyber infrastructure that is not effective. As a result, we end up adding layer upon layer of patches – but the real problem is that the foundation isn't solid. So, it can often feel like "trying to change a tire on a moving vehicle," he said. Burg agreed, noting that when the foundational software was being created, many of these issues weren't anticipated.

Burg then asked about the major threats that companies and governments are facing today. General Vautrinot replied that espionage is the first threat – not just for nation states, but also for the private sector. Company systems house valuable IP, data, and strategy, all of which are targets of cyber espionage. The number two threat, she said, is ransomware because it's all about the money. "If you can hold any portion of a company hostage, that is a business base in itself," she said. Vautrinot added that companies will soon begin to prioritize control systems or

‘SCADA’ (supervisory control and data acquisition). All major and minor infrastructures have control systems, she said, and control systems are discoverable. Charlie Leonard added that he views attacks on critical infrastructure as one of the most glaring threats. But, he added, understanding these threats is just a first step. The question is: “How do you build a system that quickly recognizes a threat and enables you to adapt?”

Bringing the discussion back to the board room, Burg asked what perspective directors should have about cybersecurity. Vautrinot suggested that she first views cybersecurity from a business perspective and operational risk perspective. The focus now, she said, is a unified system approach. For example: when you build a new building, ask if/how your cyber and technology teams are involved. Leonard agreed, adding that it’s not a technology risk issue, but rather an enterprise risk issue. It’s not about buying ‘whiz-bang’ technologies, he said, it’s about people, processes, and policies.

Following up, Burg asked about the difference between compliance and security. Leonard argued that a compliance-first focus is often not helpful because it can become a box-checking exercise. Compliance is *not* security, he said. Instead, he advocated focusing on security and resilience first. Having done so, you will have gone a long way towards achieving compliance because, although regulations are increasing, most regulators are demanding the same things.

An attendee then asked about the value of having a ‘digital director’ on the board. Leonard responded that it’s not necessarily a bad idea. But, he added, there’s a risk that the rest of the board will defer to that person. Kelly added that boards don’t necessarily need someone with deep cyber expertise. But boards do need someone savvy – and brave – enough to ask the right questions. The value of having a technology expert on your board, he argued, is that they’re likely to go deeper, and question management more frequently. As a result, someone with deep technical expertise on board can help to catalyze the discussion. Vautrinot agreed, adding: “If you can have a discussion, it sparks a debate, which facilitates a decision.” The board and c-suite need to have depth in their discussions, she said. Talk with your C-Suite ahead of a meeting, she suggested, so they know what you’re interested in and what they can cover that would be helpful.

Burg asked the panelists what best practices or advice they could offer. Leonard suggested looking into Safety Act Designation offered by the NSA and DHS. Not only can it help you recognize potential vulnerabilities, but it also can provide a liability shield in the event your company is attacked. Vautrinot agreed, noting that the inspectors come in for free, and don’t have reporting requirements like in other areas of government. She also suggested hiring someone to explain and explore the Deep/Dark Web for your company. There is a lot of activity out there, she said, and your company should at least be aware of the space. Kelly added that there is a lot of personal information there too.

Finally, Burg asked the panelists to summarize their key takeaways. Vautrinot emphasized having 'smart conversations.' Don't let jargon that you don't know go unchallenged. Force management to make you understand. Technology is admittedly daunting, she said, but it's not insurmountable. Kelly offered three takeaways. First: don't be intimidated; trust your intuition. Even if you ask an inelegant question, the important thing is to get the dialogue started. Second: go to the margins. Chief Security Officers often run the conversation, he said. If the CISO gives you the company's top four priorities, then ask what number five was and why it didn't make the list. This can draw out some interesting discussion. Finally: recognize that you're in this for the long haul. There is no short-term fix, so start viewing cyber as a process of continuous improvement. Leonard observed that every company is different, and you must match your approach to your particular business risk. That said, he suggested exploring the NIST framework as a starting point. Get someone to explain how NIST applies to your company, what you're doing now, and what you should be doing. Finally, focus on liability mitigation strategies like the Safety Act Designation, well-tailored insurance programs for cyber risk, and commensurate D&O protection.