The Cybersecurity Framework

An Interview with David Zacher,
Executive Director of ONG-ISAC and Cyber Risk Specialist Leader with Deloitte & Touche LLP

EDITORS' NOTE *David Zacher has held his current post since February 2016 while also a senior manager with Deloitte Advisory Cyber Risk Services. Prior to joining Deloitte, he served for eight years as Chief Information Security Officer for a major oil and gas company. He has served as Chairman of the American Petroleum Institute IT Security Subcommittee (API ITSS), and was a founding member of the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC). He has also been Manager IT Security, Risk Management, Compliance and Access Administration for Marathon Oil Company; Director of IT Development and Quality Assurance for Dohmen; IT Audit / SOX Implementation for Dell; and did IT for BP. He received his B.S. in Computer Science from University of Missouri-Columbia.*

David Zacher

CENTER BRIEF *Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC; ongisac.org) has been created to provide shared intelligence on cyber incidents, threats, vulnerabilities, and associated responses present throughout the industry. Building off the best practices in other sectors and fusing that with deep knowledge of the oil and natural gas industry, the ONG-ISAC serves as a dynamic cybersecurity hub for members to communicate and coordinate.*

COMPANY BRIEF *Deloitte (deloitte.com/us) provides industry-leading audit, consulting, tax, and advisory services to many of the world's most admired brands, including 80 percent of the Fortune 500. Their people work across more than 20 industry sectors to deliver measurable and lasting results that help reinforce public trust in their capital markets, inspire clients to make their most challenging business decisions with confidence, and help lead the way toward a stronger economy and a healthy society.*

What excited you about joining Deloitte and how has your role at the firm evolved?

What attracted me most was the quality of people Deloitte attracts and how they leverage those individuals to help other companies.

Deloitte doesn't focus on just the bottom line but the long-term outcomes and getting those things right.

We help clients with their risk strategies by helping them understand the technologies and how they have evolved over time. We help people figure out how to best guard or protect assets, and to do that from a business perspective so that companies are able to achieve their overall business goals.

It was very important to me given the role that I was in to help become the bridge between the IT organizations and the business. Deloitte seems to know how to do that and has the know-how to approach any type of engagement.

Many see the CISO role from a tech standpoint, but how do you define an effective CISO today and is it as much about strategy as technology?

It's definitely about strategy and how one can apply risk management to help the business still achieve its business goals while giving them the confidence that risk is mitigated to an acceptable level. It will never be completely gone but we have to make sure they're aware of what the risks are and let them make the decision for their organization on what a risk looks like. We are able to translate that into language that IT folks can understand and then react to and do the same for the C-suite and the board.

How critical is it to openly share information when it comes to addressing the challenges and threats?

There is quite a focus on information sharing and it comes in two categories: there are things that help to decide if a company is moving in the right direction from a strategic standpoint in terms of what they're doing to mitigate threats and attacks from bad actors.

There is also technical information out there that we're trying to get to be more actionable. The real challenge is making sure that the information that is being shared is not bogging people down. Companies now want to share with each other and they don't see it as a competitive disadvantage to keep everybody secure. It's about getting the right information in the hands of the people who need it, whether they're creating strategy or doing some type of tactical maneuvers.

Is this a concern across all industries?

Companies are working to understand risk but the risk continues to evolve and include factors that weren't there in the past.

We're only as strong as our weakest link and the oil and gas supply chain is quite massive. It involves large and small companies and they can easily have relationships with each other from a supply chain perspective. The companies are somewhat integrated with third parties and we have to ensure the third-party security is not the weak link.

With the information sharing today, the basic concept is to allow those who have the capabilities to detect potential threats to share that threat intel with other companies who may be exposed to those same threats but don't have the right tools to detect them. That's how we collectively keep our communities secure.

How critical is it that boards be involved in these efforts?

It's extremely important. Security has to become part of the corporate culture and awareness of the cyber risks facing an organization begins at the top with the board, not just the C-suite. The expectation has to be that a company will plan for resiliency across the enterprise and that begins with a proactive approach and awareness of the risks facing the organization.

Is the conversation today still focused around addressing a problem after it occurs and what is being done about prevention?

The conversation needs to be touching on all of the issues that we see in the cybersecurity framework. This includes not only what assets an organization has and what is being done to protect them, but also capabilities to detect whether they are either vulnerable or have been exploited by bad actors and then they need to be able to prepare for and then react to those threats with some type of response mechanism.

There will always be an opportunity for a vulnerability to be exploited, but we have to detect it as quickly as possible and have mechanisms in place to respond to it and recover from it.

Most of those responses have to be practiced so they become automatic because what is required in a response scenario is often not likely what instinctively one first chooses to do. At Deloitte, we lead cyber and crisis war-game simulations for clients and organizations so that they can develop the confidence in their incident response playbooks and make planned actions as quickly as possible, and that everyone involved understands their roles in an incident.

There are always lessons learned that come out of those response drills that can help a company refine their mitigation strategies and identify strengths and vulnerabilities.

From an ONG-ISAC perspective, from an information sharing standpoint, sharing possible mitigations for particular threats is important for supporting and promoting the industry and its future success. ●