Security Leadership > Next Generation Security Leader >

Intelligence and Resilience in Next Generation Corporate Security

By the Security Executive Council

In September 2021, the SEC hosted an online event, Reimaging Risk and Security for Next Generation Resilience. The two-day virtual research and development forum featured an impressive panel of SEC staff, Solution Innovation Partners, academic partners and leading security practitioners eager to discuss operationalizing and optimizing people, process and technology for future risk mitigation value.

Here are a few key takeaways from Day 1.

- The convergence of corporate and cyber security is often said to enhance resilience by broadening the view of risk, providing rapid detection and response to issues, and improving intelligence sharing. But we have no hard data to help us measure it or verify its benefits, drawbacks, and evolution. The SEC's Security Leadership Research Institute and Kennesaw State University is conducting a study to provide new insight into the practical side of convergence, and we covet your input. Are your operations converged, semi-converged, not converged, or considering your options? Click here to take the survey.
- Organizations can't be future proof, but with strong intelligence capabilities they can become future capable, meaning they can learn to identify and interpret the signs of coming change for a robust response.
- COVID has changed how resilience is viewed organizationally, because this crisis isn't owned by one function or leader. Whole organizations have had to work together. This can inform how we think about risk and resilience issues moving forward.
- Intelligence and analysis teams have become instrumental during the pandemic, and the appetite for information won't abate once the COVID crisis ends.

- The next generation of security leaders will have to be experts in much more than security. We will have to learn the entire business to anticipate how emerging issues will broadly impact the organization.
- All organizational units are well served by good policy formulated on good information. A solid internal intelligence function may comprise a 70-seat fusion center or a couple of dedicated employees, but they must have reliable data sources.
- Ontic's 2021 State of Protective Intelligence study surveyed 300 physical security decision-making executives. Of those who had seen a physical threat against an executive come to fruition, half reported that the event could have been avoided by better collaboration between corporate and cyber security.
- Organizations now have access to a daunting amount of data, but too many are still reacting to events rather than using that data to hunt for potential threats.
- When developing a fusion center or GSOC, begin by asking what data you want to collect, and understand how fusion technology and data can be used for more than one purpose.
- A fusion center or GSOC can be viewed as a central nervous system through which to process and distribute physical and platform security signals. Develop your own signal collection requirements, and categorize your fusion center activities – fundamental, essential, adjacent, or nonessential.
- Focus on how you add value. Recognize what the company's key services are and support those. Be ready to show the value of cost avoidance.
- Security produces oceans of data, so signal-to-noise ratio can be quite imbalanced. Tune it to enable informed decisions for all business units. Use the data you collect to tell a meaningful story. You're a curator of information. Visualize and map.
- Fusion centers or GSOCs don't have to require Fortune 100-level resources. You can use off-the-shelf tools and data sources if you don't have a formal internal intel team. Don't forget to find out what data you have in house already.
- Security should not be a competitive advantage. We should all be ready to share risk findings with the broader community.

On Day 2, SEC Faculty, next generation security leaders, students, and Solution Innovation Partners (SIPs) shared additional case studies on leveraging service and technology innovation and integration to drive people, process, and all-hazards risk mitigation for continuous improvement.

Thirteen of the SEC's SIPs presented their latest innovations to the audience in a 10-minute, Shark Tank-style format. Attendees were shown interactive, forward-thinking services and technologies that could be adopted across their entire enterprise. The 2-minute Q&A sessions after each presentation were lively and informative, with attendees gleaning details from presenters on adoption, open architecture integration, and return on investment.

One Chief Security Officer commented – "I really appreciated the format of hearing quick headlines on the product/service for many companies in one sitting. More efficient way to stay on top of what's new out there."

For information about the SEC SIP program and SIP case studies, click here.

Visit the Security Executive Council web site to view more resources in the Security Leadership: Next Generation Security Leader series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com