Career Intelligence

By Jerry J. Brennan
Contributing Writer

The Role of Intelligence in Corporate Security

Several of my recent security recruitment projects have been for clients who have asked for advice on whether their corporate security programs were aligned with current trends. They want to validate they have the correct focus, structure their security roles to support it and then hire the right people to fill the positions. They require a certain kind of intelligence.

Intelligence is certainly not an unknown to security professionals. Many spend their careers in pursuit of information that will keep their organizations secure. All companies require intelligence to stay ahead of new threats and improve their resilience. Diligently gathering intelligence and correctly analyzing it is a route to clear decision making in both business and hiring choices.

There is an expectation for quality, timely and well-presented intelligence as a deliverable from corporate security. The fast pace at which threats evolve make it difficult for companies to keep pace through the achievement of optimal security department architecture. As a result, organizational structures, security roles and their responsibilities vary widely.

Regardless of where positions report, expansion of intelligence-related roles continues in several areas:

- **Emerging Cyber Threats** – Organizations are expanding their security functions to include a wide variety of roles to meet new cybersecurity standards and industry specific regulations. Predictive intelligence is required to ensure risk management and resiliency.
- **Geo-Political Risks** – International political conflicts threaten both the financial and operational stability of organizations. Companies require a framework to mitigate these risks and are looking for security professionals to structure them.
- **Due Diligence** – Validating the integrity of an organization's supply chain remains an integral part of security management. Company mergers and joint ventures are announced every day, and these activities require people with additional due diligence expertise.
- **Competitive Information** – Intelligence continues to inform current and new corporate programs. Cross-organizational information sharing requires security professionals who have an appreciation for a broad business scope.
- **Counter-Intelligence** – Raised public awareness of the security measures organizations should have in place ensures ongoing critical analysis. Security professionals who can conduct in-depth vulnerability assessments across the enterprise remain in demand.

Together these areas are at the core of many corporate security risk management programs. Security executives who are called upon to lead them must be business leaders who manage sophisticated intelligence programs. They must be skilled at communicating with senior leadership as the information evolves. Security's return on investment relies on intelligence. S

About the Columnist

Jerry Brennan is CEO of the Security Management Resources Group of Companies (www.smrgroup.com), the leading global executive search practice focused exclusively on corporate and information security positions.