While security professionals are acquiring advanced business degrees in significant numbers now, many still bring a technology mindset, and a background in computer science, to the profession. This makes them excellent security practitioners, but less natural project leaders and strategic business executives. Security leaders have the best intentions to align security to business goals, but without a proven model or business methodology to follow, success may get lost in the tactical efforts required to keep up with the onslaught of evolving threats.

In the security organization, heads are down and focus is on putting out the next fire. Professionals are not always able to take the time to think strategically about their security programs and how best to implement them.

Here we outline key takeaways from business and academia methods that help security professionals prioritize efforts, recognize and respond to progress and maintain consistent focus on the grand end game.

Method:	The Kellogg Innovation Framework (Northwestern School of Business)	Lean Process Management	Stanford University's Design Thinking
Description of Method:	According to Dr. David Reis (SVP & CIO at Lahey Clinic), the Kellogg Innovation Framework, "helps you develop an innovation engine for reacting to today and preparing for the future."	Lean organizations are agile, adaptable, healthy and smart. Lean businesses create high value processes at the lowest overall cost. In lean organizations, value is created as the process is fine-tuned over time.	"Design-thinking" makes empathy a part of the innovation process.
Key CISO Takeaways:	o Use the framework to ensure your "security program makes forward-looking progress, while dealing with near term issues," says Reis. o Instill an innovation mind-set in your team to develop creative security solutions that enable business.	o View security programs as cyclical processes, not linear to ensure continuous evaluation and fine-tuning of security processes to provide the maximum value. o Lean process management discourages distractions and keeps the security team focused on business alignment.	o Design security solutions that deliver a positive, even transformative experience for users. o Regularly evaluate security programs in relation to how they impact users.