Infosecurity **Magazine Webinar Report**

Security Frameworks: How to Spearhead Careers & Bolster Cyber Defenses

Sponsored By

#InfosecWebinar
@InfosecurityMag

On Thursday June 28, Infosecurity Magazine hosted a webinar in association with Immersive Labs exploring the role that security frameworks such as ISO 27001/27002, NIST, and MITRE ATT&CK can play in both advancing infosec careers and bolstering an organization's security defenses.

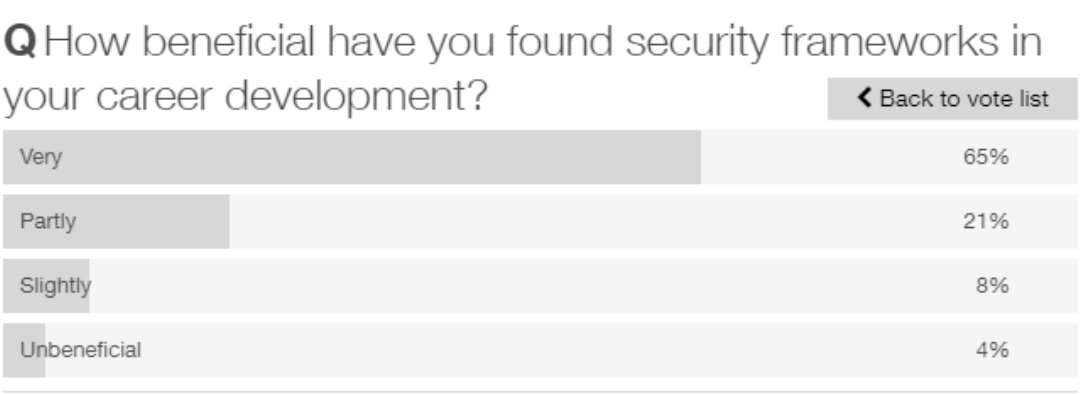
A panel of industry experts gathered to discuss the various security frameworks currently on offer, reflect on the challenges individuals and businesses can face when it comes to selecting the best frameworks to follow, and outline how frameworks can be utilized to underpin improved security baselines and maximize workforce development.

Speaking first was Sarb Sembhi, CISM, Virtually Informed, who explored the need for strategic thinking and business-value/risk management consideration when choosing the right security frameworks for purpose.

Sembhi added that alignment is also an important factor, because "security is, in many respects, a people business – we mustn't forget that and we need to think about the people that work in our teams and skilling them. If we want to keep our staff, we must be aligned to their needs for career paths and career progression."

Sembhi explained that the positive thing about security frameworks is that there are a great many to choose from, and suggested a number of key considerations when selecting which frameworks will be the best fit for either career development or the wider business.

#InfosecWebinar
@InfosecurityMag



Results of audience poll question 1

Speaking next was Raef Meeuwisse CISM, CISA, author of Cybersecurity for Beginners and various other security publications, who explored both the benefits and potential challenges of security frameworks.

Meeuwisse explained that security-by-design or DevSecOps strategies require an organization to establish a consistency in identifying risk from the outset. Security frameworks, he added, provide the benefits of a consistency of approach, the discovery of previously unknown vulnerabilities and risks, and the ability to leverage the work of many others.

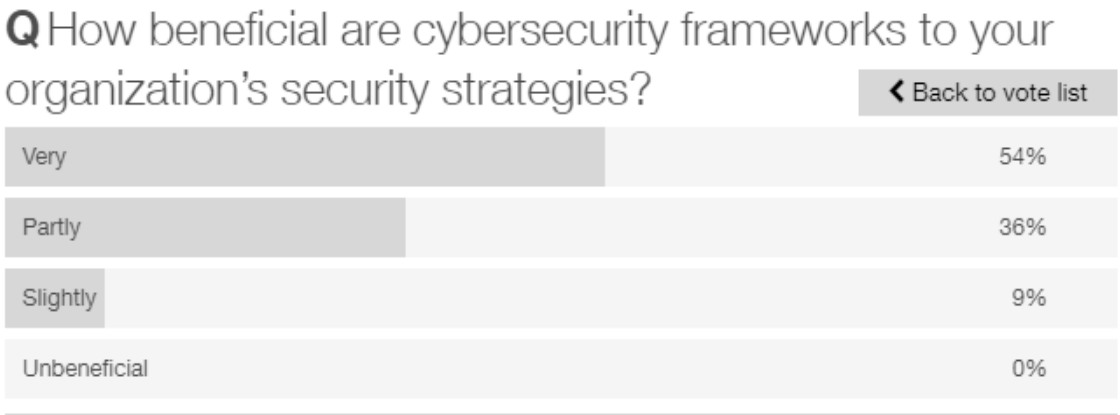
However, Meeuwisse added that "each framework has different qualities," and that potential confusion [can arise] when multiple frameworks are in use.

"Often, organizations are using a dozen or more different frameworks for different purposes," he said. "There is a lot of potential for confusion when, especially in large, global organizations, you end up using vast amounts of frameworks."

He also pointed to a “lag between evolving threats and new controls appearing,” which can be problematic, because some frameworks can have a limited lifespan of effectiveness.

To conclude, Meeuwisse reminded the audience that “one size does not fit all” when it comes to security frameworks, and there are many considerations that are likely to impact the framework focus you have.

“A good way to think about frameworks is by thinking about tools,” he added. “You wouldn’t pick up a mallet to do a job that needs a screwdriver, and it’s the same with frameworks. The selection process of a framework and understanding what you’re using is absolutely vital.”



Results of audience poll question 2

#InfosecWebinar
@InfosecurityMag

Speaking last was Max Vetter, chief cyber officer at Immersive Labs, who discussed some specific frameworks that Immersive Labs has been successful in using to both help train and upskill staff and to improve cyber-defense within the company.

Vetter first cited the NIST National Initiative for Cybersecurity Education (NICE) framework, which aims to energize and promote a robust network and an ecosystem of cybersecurity education, training and workforce development.

“What NICE really tries to do is map careers to the knowledge that you need within cyber and then you can use that to understand what kind of careers you have,” he said.

“We have taken our 600 labs, mapped them to about 600 knowledge areas, and then put them within our platform, where you can select any work role. It’s really all about understanding career development through a cyber-lens.”

Immersive Labs has also been successful in working with MITRE ATT&CK, Vetter continued, which is a framework that focuses on cyber-defense. “MITRE ATT&CK looks at the different tactics that attackers use” and Immersive Labs matches its labs to each, individual technique, and then gauges knowledge levels across the organization. “That gives you a good indication of where your gaps are, and that’s a big part of the point of frameworks – that they can help you find gaps in your defenses once you’ve worked through them.”

Results of audience poll question 3

As was discussed and explored in this webinar, security frameworks can play a significant role in advancing careers and improving organizational security defenses. However, selecting and effectively implementing security frameworks is not without its challenges, and requires both forethought and strategic management to get the most out of the right frameworks for the desired purpose.

This live webinar was broadcast on Infosecurity Magazine's Webinar Channel 27th June, 2019 and is now available on demand - https://www.infosecurity-magazine.com/webinars/cyber-defence-webinar

#InfosecWebinar
@InfosecurityMag