JUST DON'T DO SECURITY

Do you want to support your organization?

Don't just do security!

Wait, what did you say will be one of the first questions you could ask, but I am a security professional! I do security! I get it; security practitioners, we do security, so why am I starting with that statement? Well, that is what we will figure out in this brief document.

Recently I was reading "Una Segunda Oportunidad" (A Second Chance), written by a prestigious security professional, Mr. Hector Coronado, CPP. He mentioned that at the beginning of his career, he was focused on "extinguishing fires" without a clear methodology and a widespread mistake made when talking about risk management is when we think that risks only are owned by Security and, of course, it is not the case in any company. Reading about his experience, many experiences of my own crossed my mind. It was like a movie that had popped up, many lessons learned and for sure, many mistakes and probably a very similar "bushfires" that I had extinguished just like Mr. Coronado.

As security professionals, want to be successful and protect everyone and everything; believe me, that is when we need to stop and don't do just security. Understanding the business comes first! What are the organization's goals and strategies? How do your stakeholders think and act? How do you establish a strong relationship with them? Do you truly understand their needs? How does your functions affect their operations? A while back, I heard from security practitioners say "I'm just an operational actor here; I don't have anything to do with the strategy" ... Wrong! Even if your position is fully operational in nature, your OKR (Objectives and key results) must be aligned with the organization's strategy! Otherwise, you will be just an expense without true value for the company. Your actions probably will affect others more than helping them, adding barriers to the operation rather than protecting them.

One of the first things that you must do, whether it is your first day in your new job or you have been working in a given company for long is to understand the company strategy. If you do not know or understand the company strategy, you need to find a mentor, a coach, etc. or anyone in the company who will teach you about it. He or she should be able to create impactful OKRs, which are aligned to the plan. Secondly, you need to establish a bond with the other functional areas. This will include your stakeholders (internal and external clients). Additionally, map out the interaction and the processes, which will allow you to understand where there could be any pain points or room for improvement. Thirdly, in a team-working environment, ensure you reach an agreement with your stakeholders for the KPIs that will measure the impact of your function, team, actions, etc., on their operation. Additionally, you need to establish SLAs that will help you to have time to work and not be a "fire extinguisher," focusing on yourself and your team in urgent matters that are not necessarily urgent in nature.

Well, I have got that already covered! Can I do security now? Wait, do you have your risk identified as well as the risk owner? Understanding the risk, who owns it, is very critical to saving company resources. It ensures there are no headaches for you and helps focus on what is essential to ensure the company's business continuity.
I recall a while back when working at Google Datacenters Security Team. In this team, we were thinking about initiatives that would help to create or develop a security culture among the other functions. A good friend of mine, Mr. Wade Meadows, Security Manager for Lenoir Datacenter in North Carolina, USA told us about a meeting that he had with the site management where he was asked about something to encourage Google to align with security procedures, he quickly responded **#DoSecurity!** Besides the laughter and open responses from others, **#DoSecurity** was established as "the way" for everyone. This was established, keeping in mind that acting according to the security policies and procedures was important to ensure the Datacenter business continuity. This was possible, not because of the intelligent and bright mind of Mr. Meadows, but because the entire organization already had a clear picture of the risks that could affect the business continuity. They were working as a team and thanks to Mr. Wade Meadows, they were aligned to the policies and procedures needed to mitigate any potential events that could impact the operation.

In summary therefore, we need to focus on the business, understand the strategy and our stakeholders' needs. Additionally, we need to understand what are the risks and their owners. Once this is achieved, then and only then, **#DoSecurity!**

Alvar Orellana McBride, CPP
ASIS International RVP Region 8C
Executive Director, Griffin Risk