Cyber Security as a Cost-Inefficient Infinite Game

In his book, Simon Sinek wrote “How do we win a game that has no end? Finite games, like football or chess, have known players, fixed rules and a clear endpoint. The winners and losers are easily identified. Infinite games, games with no finish line, like business or politics, or life itself, have players who come and go. The rules of an infinite game are changeable while infinite games have no defined endpoint. There are no winners or losers--only ahead and behind. The question is, how do we play to succeed in the game we're in?”

The honest answer to this question is that there is no such thing as ‘winning’ in the cyber security game and this is where most organisations and people that work in the sector make the biggest mistake. When viewing cyber security as a finite game with an endpoint, you are only focusing on reaching an endpoint that will never come and becoming the winner you will never be.

Because an organization is playing an infinite security game where there is no level playing field, it is very important to optimize the cost-efficiency and effectiveness of the security measures implemented, however many organizations fail to do so. Currently one of the most used frameworks to tackle gaps in cyber security is the so-called ‘NIST Framework’. In this framework, it is stated: “Set cybersecurity goals for the organization, identify gaps between current practices and the goals, and plan how to address the gaps in a **cost-effective manner**.”

It is important to make cyber security investments cost-efficient and effective because organisations have limited resources such as budget, personnel and time. Ensuring cost-efficiency in cyber security can ensure that the budget can be allocated to other operational important processes such as innovation and product development, which are most of the time more important for an organisation than cyber security. Next to that, cost-efficiency in cyber security will ensure the right investment that will lead to the most optimal risk mitigation. Cyber incidents can for example lead to financial losses, legal liabilities and reputational damage. Implementing cost-efficient cyber security measures will therefore help organisations to optimally reduce the likelihood and impact of cyber security incidents, saving them from potential financial losses. Organisations must not view cyber security budgets as 'expanses' but rather as a process of investment which will return in the long run (in finance this is called ROI; return on investment).

It is also very important for organisations and businesses to make cyber security measures cost-efficient and effective as it will be easier to scale business processes. When organisations grow, the more cyber security needs to evolve. Cost-efficient cyber security measures allow organisations to scale measures in proportion to growth, without breaking the bank.

The infinite cyber security game as described by Simon Sinek cannot be won, but can be made and must be made as cost-efficient and effective as possible, to ensure the continuity of organisations and businesses.