RESILIENT CYBER SECURITY THROUGH CYBERCRIME MARKET ANALYSIS

Per Håkan Meland,[1,2]
[1)]*NTNU, Norway*
[2)]*SINTEF, Norway*

Abstract
Most cyber security compliance frameworks follow the traditional path of identifying risks in advance and implementing controls or barriers to tackle malicious attacks. Unfortunately, there is a severe imbalance between the effort of protecting a system and attacking it, commonly referred to as the *defender's dilemma*. The defenders participate in an unfair game where they need to prepare against all possible threats at all time, while the attacking side can concentrate their resources on a single vulnerability at their leisure. For the defenders, this is not feasible in the long run, so in practice, they are left in the dark, having to accept that there are many risks that cannot be fully understood and dealt with in advance.

The contribution of this paper is an approach where observations from cybercrime markets are used as sources of resilience, that is the ability to anticipate attacks, better withstand them once they occur, recover from the disturbances and evolve the protection mechanisms. Using information about the type and popularity of malicious digital goods, we can get indications about who the attackers are, when these arms are in their hands, what kinds of assets they are looking for and which vulnerabilities they are likely to exploit. Considering the economic incentives of the attackers, and not just the capabilities, can also give us an improved understanding of the risk likelihoods as historical incident data quickly becomes outdated, and in the wort case – misleading. A limitation with this approach is that it mainly anticipates attacker with economical rationality, and not those that are driven by reasons such as political change or revenge.

Keywords: *Cyber threats, risk management, cyber resilience, economic incentive*

ISBN: 978-91-88898-41-8