SECURITY FROM THE INSIDE OUT

Security | Risk | Governance

The new risk equation: Motives - Means - Opportunity

One of the simplest definitions of risk that I have found in my career is expressed in the form of an equation, with its variables, its factors, its result. This is (or was) the following: for risk to exist there must be a **threat** that uses a **vulnerability**, with a **probability** of that happening and there has to be an **impact** (**Threat - Vulnerability - Probability - Impact**). There must be someone (or something) who wants to harm, our systems must have a hole (which will be exploited by the attacker), there must be a probability of this occurring (the greater exposure and/or holes, the greater the probability) and, of course, there has to be an impact, a damage, a loss (otherwise, we could talk about residual risk or even existing risk without real consequences).

Taking into account the previous equation and with the aim of mitigating that risk, we can only work on three of the four variables that build it. We can only reduce the **exposure factor** by reducing existing **vulnerabilities**, by closing those holes; in doing so, we will naturally reduce the **likelihood** of an attack occurring and that is also working on the dimension of dwarfing the risk. And protecting the assets with the appropriate countermeasures - always knowing the value of what we want to protect - we will be reducing the **impact**. Fantastic. However, what we cannot avoid is that there are agents who want to cause evil, who want to steal corporate information and/or who simply want to cause disruptive situations for the entity. We cannot avoid that there are malefactors (beyond social and educational policies for society that are not subject to these lines) and, consequently, we must comprehend that the threat factor, with that external element - usually- that wants to damage the reputation or economic-financial situation of an organization will always exist and we can do nothing about it.

Reflecting on that factor over which we have no control of the risk equation, another 'equation' came to my mind that could well be an explanation of why these threats exist and why the society in which we live experiences an amazing increase in some types of threats -1500%- (no, not a typo) as with *formjacking* and other innovative attacks. It's about **Motives - Means - Opportunity**.

A digital attacker -as in the physical world- needs a reason to harm, an ultimate goal that 'authorizes' her/him to perform the action. Currently two fundamental reasons are cited: money and social or political disruption. These are the two main

reasons that move cybercriminals to perform their acts. However, if the adequate means are not available, the will to carry out an attack would only remain in the design phase ... unfortunately, though, there are very advanced means ... with costs that have dramatically reduced the ARPA (*Average-Revenue-Per-Attack*) and they are even 'borrowed' by groups of larger attackers to smaller groups sharing benefits (!). We have reached the democratization of the attacks. We have arrived to the extent of a concept taught in first year of Business and Economic Sciences: a cartel (an organization that reaches agreements with other companies in the sector -the bad ones- and eliminates the competition -the good ones-).

Finally, in this new risk approach, attackers need a window of opportunity, which does root with the 'old' risk equation in its facet of exposure factor, company visibility, vulnerability management, ... The Internet allows the invisibility of the attacker ... or if there is visibility, the international judicial system does not always facilitate the prosecution of the crime. Thus, the opportunity aspect is as relevant as the other two factors.

If we add sophisticated **Tactics, Techniques and Procedures** to this mix (TTP is the acronym), sometimes even using mechanisms that are used for protection (let's not forget that the main pillar of ransomware attacks is the encryption of the data), we are facing a situation of weakness in front of these attacks.

I would not like to end these lines without addressing a positive aspect of all this: these **Motives - Means - Opportunity** are also available for those who want to **PROTECT and DEFEND**. Today, companies know the reasons to safeguard information - not only the law but common sense should play an instrumental role here-. They have the means to do so (obfuscation in the use of the cloud, isolation chambers, safe navigation, encryption of communications, etc.) and, above all, the opportunity. There has never been so much information or technology to perform that protection and defense effectively. You have never had so much threat intelligence - captured with millions of points of information at the endpoint, in the network, in storage cabins, in the gateway, in mobile devices, ...). Therefore, there is a 'new' risk definition with new variables to consider: **Motives - Means - Opportunity**. For the bad guys ... but also at the reach of us, the ones who have to defend. We, the good ones.

Ramsés Gallego (CISM, CGEIT, CISSP, SCPM, CCSK, ITIL, COBIT, Six Sigma Black Belt) is Security, Risk & Governance International Director with Micro Focus