An industry colleague who attended the 8th July NZISF Seminar, in Auckland, raised the below question:

Hi Gabriel,

Good morning. Thanks for making your presentation slides for NZISF available.

I have put a bit of thought into your formula Risk Profile = sum(Threat * Vulnerability - Control).

For me, risk is associated with entropy (the uncertainty or chaos), which can only increase. I don't feel comfortable with Risk Profile being potentially 0 or even negative.

Perhaps, Bryce's suggestion may be useful: sum(Threat * vulnerability / control) = Risk Management coefficient.

Anyway, it is just my naive opinion for your teatime. Please do not worry about it too much.

Have a great day.

Best regards,
Aria

Response below:

15th July 2021

Hi Aria,

I am glad to hear you created some time to reflect on my presentation. THANK YOU.

I did send an update to the presentation slides via Lech. Please see additional attachment to this email. The Summary below.

#	Models	Static Views
1	Associative	Risk Profile = ∑(Threat * Vulnerability **-** Control)
2	Conjunctive	Risk Profile = ∑ (Threat * Vulnerability **/** Control)

You are absolutely right that risk is about degree of uncertainty and entropy – randomness. In fact, that is the whole point of the SVRE. I presented the abstracted (simplified) version at the NZISF as a primer to introduce the concept. The core of the SVRE is the application of Field Theory to solving for the uncertainty in business environment. Path Integrals are a core tool and if you are familiar with Quantum Field Theory, you will see the correlations.

Also, you are correct in that negative and/or zero risk profile sounds a bit odd. That is very apt. If you recall, I started the presentation by suggesting and linking the whole essence of business existence to the presence and effective management of risk. So, if risks were to become negative and/or zero, the business has no moral right and in fact could not exist.

Let us look at the two models above and see what kind of situations may lead to zero and/or negative risk profiles:

1. **Associative**

   Risk Profile = ∑ ((Threat * Vulnerability) **-** Control)

   In this risk model Risk Profile can only be zero/negative if one, on aggregate, implemented too much controls, equal or greater than the quantum of risk in the environment. If you reflect back at our discussion, controls implementation require investment (cash, emotion and political capital). If excessive controls are implemented this will create a negative/zero risk profile, and the business will fail. Naturally, the Board of Directors, through the company management will eject the risk management operative before the business is grounded to a halt. This is one of many reasons, a technically sound security professional may not be effective in some given business environments; and they may be asked to leave.

2. **Conjunctive**

   Risk Profile = ∑ (Threat * Vulnerability ***/*** Control)

   In this risk model Risk Profile cannot be zero but could become infinitesimally small and insignificant, to be assumed as zero, if excessive controls are implemented.

   This scenario will lead to about the same outcome because the bottom line of the business will be eroded, which in and of itself defeats the cardinal purpose of security.

General view

A. Whilst model 2 (Conjunctive Model) appears easily digestible, especially, if one was new to the SVRE [I know that may sound cheesy as the SVRE is new], it is a bit of risk on its own. Why? The reality check is lost. Because if one does not get that immediate inversion signal (zero/negative), one may continue down a self-destructive path.

B. The beauty of the SVRE though is that the issue in (A) above is immaterial, because what the SVRE looks into is the change and rate of change in risk dynamics. Please have a look at the supplementary notes forwarded post presentation and notice the following:

   I. Both Associative and Conjunctive Risk Models lead to Risk Dynamics being dependent or functions of change in threat, change in vulnerability, and change in controls maturity;

   II. The Associative Risk Model, does however, provide some easier to compute insights more readily than the Conjunctive Risk Model. With computing resources though, both lead to the same consistent outcome.

C. Overall, my recommendation, as discussed at the meeting, is select an approach and stay consistent and true to it. The SVRE will lead to a more business driven risk management for technology professionals.

I will be happy to arrange a time for us to catch up and chat about this. I am really honoured and impressed that you took the time to reflect on my presentation.

Sincere regards

Gabriel Akindeju