Lessons from Prometheus (and simple humans)

Before Prometheus gave man his first fire, our evolutionary great-great-grandparents already had two feet planted firmly on the ground. Big-brained bipeds with opposable thumbs, sophisticated enough to begin developing instincts so vital, we still carry them today. An innate ability to identify a threat *before* it ate you was one worth keeping - something you could pass down to the kids - along with the thumbs.

Several species and four hundred thousand (or so) generations later, we are no longer on the menu, but we still face potentially dangerous and threatening situations. Keeping us safe remains the top priority for an instinct that took millions of years to develop and may take as many to alter. As we pass it on, it sometimes changes its name, but its nature remains the same.

For ICTS Europe, keeping safe is more than an instinct – it is our mission. Rapidly becoming a leading force in securing data centres, we expanded our services to some forty data centres across six European countries in the past two years. A growing number of Colocation and Hyperscale operators now talk to us about their challenges and how we can help them achieve effective and cost-optimal physical security.

This conversation is critical as data centres increasingly seek specific security expertise to match the risk profile they are facing. So, we asked our clients a simple question:

What are the most valuable qualities and attributes they would expect to find in their physical security providers?

We offered five options to rate, and the result was strikingly consistent! As shown, the vast majority scored two attributes high above the rest.

It is interesting to note that the highest priority - *trustworthy & dependable* - is all about human qualities. Possibly not that surprising, as research indicates most security failures in data centres are caused by human error in one form or another. So it is only natural that data centre security professionals value a physical security provider they can rely upon and trust.

Equally noticeable is the emphasis on the ability to *increase compliance & resilience*. First, data centres want to see *improvements* on what they were able to achieve in the past. Simply maintaining quality and reducing costs is no longer sufficient.

As threats develop, risk complexity intensifies, and as colocation clients increase their demands, data centres have to push security performance ever-upwards, which necessitates both *compliance* and *resilience*.

As a means of measuring inputs, compliance is vital, but it is only part of the broader performance picture. Resilience represents the new Holy Grail- the critical output that data centre security (physical and cyber) is judged on.

Human qualities and the capacity to drive service outputs upwards – that's what data centre security professional are telling us they need. Experience, cost optimisation, technology, and innovation retain value when such capacities serve an ultimate purpose and are not chosen at the expense of working with people you can trust.

So, let's talk about trust.

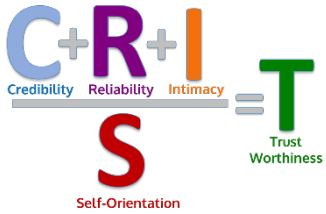
With its variety of definitions, our concept of 'Trust' plays a part in every interaction. It guides decision, shapes expectation and influences conscious behaviour.

Instinctive trust interacts directly with our primal brain – the structures which control automatic self-preserving behaviour and determine our ability to detect and respond to threats.

Our capacity and ability to trust are rooted here. These structures enable us to differentiate between threatening and non-threatening, strange or familiar. In an instant, we *spot the difference.* The unfamiliar or unknown we treat with more caution or suspicion until we have assessed it in context.

Although instinctive trust is difficult to quantify or measure, Maister, Green & Galford believe we can calculate how *worthy* of trust we are. In their business classic The Trusted Advisor (Free Press, 2000), they assign notional values to behaviour patterns relating to:

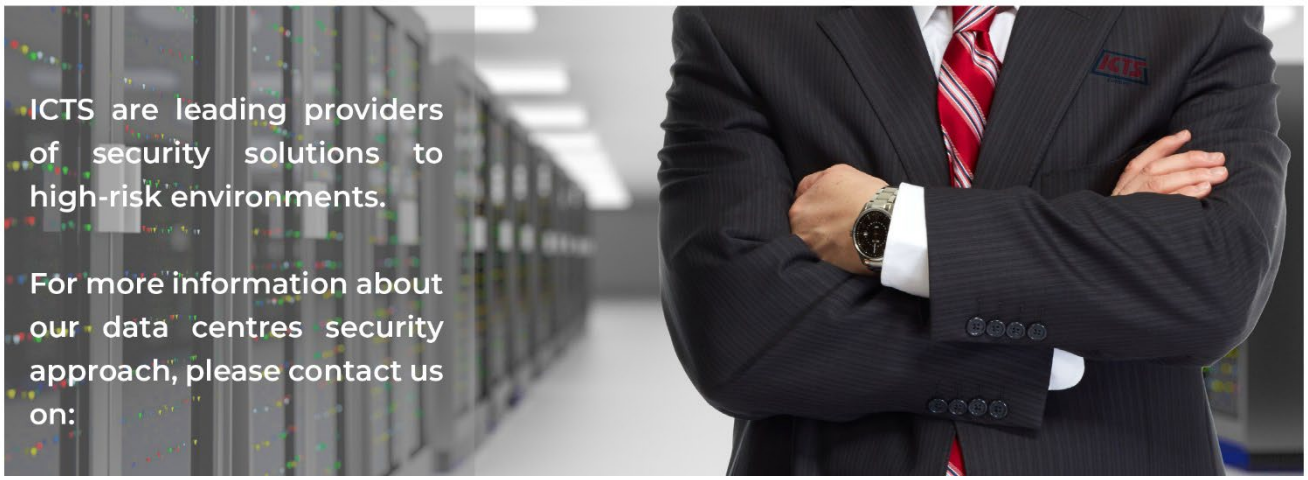
Credibility in terms of what you say and how you say it; **Reliability** in terms of what you do and when you do it; **Intimacy** (or empathy) in terms of how comfortable or safe you make others feel; and **Self-Orientation** - the extent to which you are focused on yourself. Expressed as an equation, we can see how it works:



To build trust, we need to add to our Credibility, Reliability and Intimacy behaviours. Below the line, we need to focus our attention outwards and minimise self-orientation. The sum of which is trust-worth.

Or, in our world of data centre security, trust means professional credibility, operational dependability and intense client focus.

Promethius could probably show us a few things about trust *and resilisance* - if the legends and stories themselves can be trusted. Even as a myth, there are lessons to take, not least of which is to consider very carefully where you place yours.



Garry.Malone@ictseurope.com

ICTS EUROPE

www.ictseurope.com