# All.Net Analyst Report and Newsletter

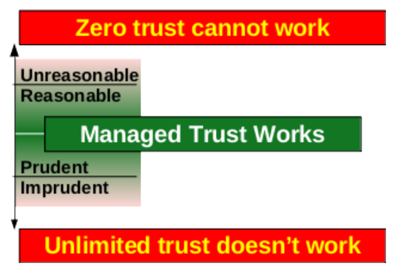
***Welcome to our Analyst Report and Newsletter***

## From ZT to MT – Clothes for the emperor

When it comes to zero trust architecture, as everyone now knows, the emperor has no clothes. The reason is simple.

- **Unlimited trust doesn't work because nothing is perfect.**
    - **It's imprudent to trust without limit.**
- **Zero trust cannot work because we trust is required for function.**
    - **It's unreasonable to try to trust nothing and no one.**

If we wish to make progress, we need to manage trust to reach a reasonable and prudent level of trust in people and things.



***Managed Trust Works***

## As a practical matter

Clearly we need to address the issues of trust and trust worthiness. And we don't really want to throw out all of the things we have learned about cybersecurity and information technology just because we are finding some of the problems we face are disrupting our longstanding and incorrect portrayal and perception of its perfection.

- **We actually have lots of effective mechanisms for managing trust.**
    - **None of them are perfect, nor will they ever be.**
        - **But the positives of cyber do and can continue to outweigh the negatives.**

## As a factual matter

Influence operations are used whenever we communicate with each other. The expression of the meme known as Zero Trust is has advantages as a mental virus.

- It's simple to say, hear, and remember.
- It's easy to spread and catchy like any other good disease of the mind.
- It requires little thought as long as you don't bother to think about it.
- Since it means nothing, you can make it mean whatever you want.
- It even rhymes (Zee Tee)

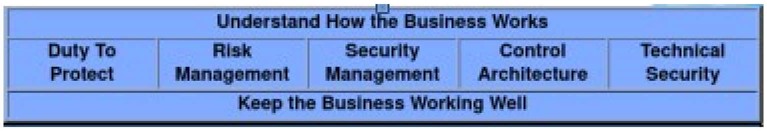
It's striking in that, at first blush, the idea of no longer having to trust anything or anyone and thereby being able to stop worrying about trust eliminates the fear, uncertainty, and doubt always being pushed on you by cybersecurity firms trying to make a sale.

It's perfectly acceptable from a political perspective. Most laws we have passed have names that are not reflective of the content. In fact, just like most laws, the names usually say nearly the opposite of what they actually produce. Did you catch that? Probably not. I'll spell it out.

- **Your distrust for politicians made it natural and acceptable to buy into the lie I just told.**
    - **In fact most laws have names that are related to their intent and much of their content.**
        - **But the names are also sales tools to get them accepted by the public**

### The architecture of managed trust (MTA)

An architecture for managing trust already exists and has existed for a long time. I use a picture here that is an example of the overarching structure of such an architecture.



Understand How the Business Works

Duty To Protect | Risk Management | Security Management | Control Architecture | Technical Security

Keep the Business Working Well

We have to start by understanding what we are trying to accomplish (objectives) and how we are trying to do that. In this depiction, we use the concept of the “business”, whatever that business might be. That understanding includes what could go wrong and the consequences of things going wrong. The mechanisms of the business are how it accomplishes things, and include people, groups, technologies, nature, and the realities of the world (the context) in which it is to accomplish whatever it is intended to accomplish.

The notion of intent is of course not simple as in an organization there may be many intents. For this reason, we define duties. For cybersecurity, we call these duties to protect (keep from harm) but more generally, they are the defined things we are required to do and not do, usually at the level of laws, regulations, ownership expressed mandates, governance, and related decisions, all of which are defined de-facto (by fact) or de-jure (by decree).

Based on these duties, the risk (uncertainty about the future) management function, which includes trust (the willingness to be harmed) management, seeks to balance risk and trust so that more uncertainty (risk) is countered by less willingness (trust). Higher risk requires less trust, and thus more assurance (things to increase certainty) of accomplishing the objectives.

Security management is the management process by which this assurance is obtained. It involves planning to meet objectives, asserting execution of the plan, verifying that the plan is being executed within identified tolerances, and acting to assert changes in execution when the plan approaches the bounds of assured execution. In the parlance of standards, this i9s called “plan, do, check, act” (PDCA). It is a forward looking feedback control system that seeks to use models to anticipate and constrain future situations, or as I have been calling it for 20+ years, “model-based situation anticipation and constraint”.

Security management operates through a set of defined models of how things work, that we will call a Control Architecture. In simple terms, the control architecture is the set of models of how things are supposed to work, and it is used do design and implement the technical controls as well as to model how they are supposed to function for comparison to how they are functioning so that performance can be measured and adapted through the PDCA process.

Technical security is the implementation of the control architecture in reality, and involves the execution of all of the various disciplines of cybersecurity which have been developed since time immemorial. And of course, the loop is closed by keeping the business working well.

### None of this is new

This is not a new invention. It is merely a restatement of what has long been known. However, in order to sell the meme of good governance, we will use the new and improved catchy name “**MTA**” – pronounced “empty – eh?” and the short form “**MT**“ for Managed Trust.

From **ZT** to **MT**. Read all the details at **all.net** → **Protection**