



Supply chain security – artificially inflated or much improved?

Security as we go about our daily business is a concept that, until recently, was taken for granted in our part of the world. However, as the events of the past few years have tragically demonstrated, this has reverted to being more of an aspiration than reality. Direct attacks on life and limb by terrorists as well as threats to people's livelihoods from pirate goods have regrettably become commonplace. Economic reasons alone are enough to motivate businesses into taking measures to combat and neutralise these threats. The authorities have been supporting such efforts for many years now by putting various tough sanctions and regulations into place.

Government actions are now to be strengthened by an initiative coming from the EU, namely the Customs Security Program (CSP) which is intended to guarantee the security of the supply chain and is due to make a major impact this year. Central to this scheme is the concept of the Authorised Economic Operator (AEO) and 'summary registration', the purpose of which is to enable cross-border risk management. Companies can – and indeed must – have themselves certified as AEOs in order to be acknowledged as having a secure supply chain. The certification process may be voluntary, but in a competitive environment, is non-certified status really an option, i.e. might there not be a domino effect? Furthermore, we find ourselves in a situation where, by the very definition of a 'secure supply chain', every single supplier or business partner of a particular AEO has to sign up to the certification process or, at the very least, sign some sort of security declaration. Is this practicable and can it be implemented in the case of a globally active company with hundreds of partners scattered across many different countries?

In order to obtain AEOS (Security and Safety) or AEOF (Customs simplifications/Security and Safety) certification, numerous hoops have to be jumped through. Expensive investments in safety and security measures become necessary, e.g. uninterrupted monitoring of premises by a system of access controls, perimeter fences and the like, as well as security checks on staff. Does all of this make sense and is it economically viable in the case of business premises that have grown organically or where services are predominantly outsourced? Can the installation of fences and access controls ever thwart the determined criminal? Are there not simply too many opportunities for introducing 'insecurity' into a long and complex supply chain? And whose fault is it when something eventually goes wrong? Even summary registration causes tremendous problems for the customs authorities and many business operators, particularly those engaged in the import trade. Huge sums have to be invested in IT hardware and software and, to make matters worse, schedules can be disrupted by an ambiguous regulatory framework.

So we are left with the question of whether the CSP can ever guarantee a totally secure supply chain. Is it not much more a case of expensively inflating the supply chain or, perhaps even worse, producing a 'pseudo-secure' supply chain that is all the more dangerous for the blind trust that people put in it? Clearly, supply chain security is an important and useful concept, provided it is handled with care and purpose. With respect to its delivery on an organisational level, the extent of the prescribed measures and the economic costs that ensue from it, we perhaps need to regard the CSP with a healthy dose of scepticism.