

A New Paradigm Applied: The Security Sector

Mark Obren, DBA

We are facing a new paradigm driven by a discontinuity induced by technology change, i.e. the separation of information from physical goods driven by information technology diffusion.

To recap, the new paradigm has the following factors:

1. enables a massive growth in wealth
2. reduces transaction costs
3. requires trusted custodians of information
4. enables new forms of organisations
5. changes the boundaries between organisations and the market
6. creates the self-interest for people to own information defining their person
7. requires maximum storage of data to realise maximum returns

The paradigm directly changes several fundamentals in the Security sector and ushers in a period where more change can be expected, with new technologies and concepts changing the way people, property and institutions are secured.

The first point is a massive growth in wealth. The change in wealth opens a gulf between those who are reaping rewards from the new paradigm and from those who are not, for a variety of reasons. In any case, the difference between different societies and individuals within the same society creates the incentive for some to use violence to capture economic and political benefits for themselves. This situation creates a need for increased security for individuals and for society against threats from those who have not joined in gaining benefits from the new paradigm.

The second point is the reduced transaction costs from the information based society enables security in novel forms, through tracking individuals and equipment, and using behaviour pattern techniques to identify potential threats. The consequence is a substantial improvement in both apparent and actual security for the individual.

The third point is that security based upon information requires a trusted custodian to enable effective security services. The information used for profiling security threats requires all parties to reveal accurate information to other parties in order to enable effective security services able to respond to actual threats. This information will only be provided if all parties trust the other parties in the transaction, and hence a trusted intermediary provides the benefit of endorsing the trustworthiness of all parties in the process.

The fourth point is that the information paradigm enables new forms of organisational structures. The reduced co-ordination cost enables disparate resources to be effectively combined to meet security threats as they occur, thus encouraging greater flexibility and use of temporary structures. The information infrastructure enables security services to operate from distant locations, thus enabling security to be provided by personnel from any location.

The fifth point is that the boundary between organisations and the market are blurred by the reduced transaction costs. The Customers of security services can use self-

service systems to provide security services, thus becoming part of the service delivery model. The use of temporary services enables an organisation to access resources as required to meet specific security threats as they arise. The concept of the organisation will evolve to include those using its systems and supporting its brand.

The sixth issue is a consequence of the sensitivity of the information used to provide security services encourages individuals to take ownership of information that uniquely identifies them. Individual-specific information can be used to create a security threat to people, and thus in their own self interest, individuals will want to deny access to that information for all unnecessary purposes. The most effective method to control information is to control the property right, and thus it is in the interest of individuals to own the property right relating to information uniquely identify them.

The final point is that the more data collected, the more the effective the security service and thus the greater the benefit to the individual and society. The optimal situation is to collect and store all data, to enable threats to be identified by comparison with historic patterns.

These changes can all be predicted by applying a new paradigm of an Information economy, but probably represent only a portion of the real benefits, many of which will become apparent only in the context of the new paradigm once it is entrenched. The consequence of these changes is a substantial improvement in the security of the average person and of society in general. However, it can be expected that vested commercial and public sector interests will resist change as it represents a challenge to the power of large-scale Suppliers and governments in controlling the security market. The ease of the transition depends on the skills and dedication of people in the sector to the consumer of their services.