Managing the Attack Surface – Axioms

→ Information security is largely about determining the organisation's attack surface, locating vulnerabilities on that attack surface and then developing and implementing an efficient and workable ongoing plan to remediate them.

→ The 'attack surface' is all of the different points on or inside an organisation via which an external attacker or malicious or negligent insider might compromise that organisation's sensitive data.

It includes Information Technology ('cyber') aspects such as computers and websites, but also non-digital aspects such as physical security and employee screening and training.

→ No organisation has perfect information security; many have a huge amount that needs to be done, but *every single organisation* has some work to do understanding and managing their attack surface.

→ Attempts thoroughly to protect the whole attack surface as soon as possible, are doomed to failure in nearly all cases.

This is because for most organisations, the attack surface is simply too large and complex rapidly to understand and manage relative to their available resources. All attack surfaces are also dynamic, with relevant assets coming, going and changing.

→ It makes better sense to step through the process in a methodical way; step-by-step, with the order of the steps planned out carefully in advance.

→ The first step of most *general* information security projects should be to identify quick wins where significant vulnerabilities can be corrected quickly, cheaply and quantifiably.

→ Vulnerabilities of this type can be identified by working through the first steps of the attack surface plan, where these steps are prioritised in terms of risk (probability and impact) and ease of remediation.

→ Quantifiable security wins can and should be communicated to (senior) management in order to secure their support for later stages of the project, which may be expensive and resource-intensive.

→ After dealing with quick wins, the attention of the project should shift to later stages of the attack surface plan.

→ All organisations can step into the attack surface plan at some stage.

→ "Doing" ISO27001, SOC2 or similar != rigorous attack surface management, although there is significant overlap; an organisation that understands and manages its attack surface really well may be more secure than one that is certified to ISO27001.