



Simple guides for your business

10 Steps to Corporate Security

1. Ensure that your Security Policies are appropriate to your organisation. The security parameters must be realistic and not simply based on a wish list of the impossible.
2. When building systems, you must treat security as an end-to-end requirement, and not just focus on a few components. For example, if you deploy a secure WiFi client, then make sure that you also secure its operating system.
3. If you employ security professionals within your organisation, you must ensure they know what they are doing, and that they understand what security looks and feels like. Only employ qualified security professionals.
4. If you deploy new systems or architectures such as WiFi or wire based remote access client then you must test them thoroughly to ensure they are secure and satisfy your security model. Do not take security for granted.
5. If you deploy a secure build then you must place it under change control. Every time you change the build you must test the entire system to ensure it satisfies your security model.
6. Remember, that your system will be used by people – the users – so ensure that you give your users security awareness training.
7. When you design, and deploy systems to service B2B, or B2C communications, you must define your desired security profile and build in security from ground up.
8. You must base system builds and their deployment on a solid Risk Assessment. The risk assessment must identify clearly any holes in the system that could be exploited.
9. If you allow inter-site communication, or remote access then you must ensure that you know and understand the security perimeter of your systems. You should identify all areas of the perimeter which could allow your secure system to be compromised.
10. If you cannot achieve your desired level of security then you need to document the remaining risks in a Risk Register which should be available all who have a business related need-to-know. You can decide to operate your system at the expense of security, but that decision should be taken and owned by a senior manager or board member.