

Information Security Assessment (ISA) Express

@copyright 2005

Top 10 Common Information Security Mistakes

<ol style="list-style-type: none">1. Presuming one line of defense is adequate – There is no silver bullet when it comes to network security. The only way a network will be secure is by having multiple lines of defense. Good network architecture starts with many layers, each layer addressing a different threat.2. Insufficient understanding of the technology, its nuances, including the multiple approaches a hacker can utilize – Knowledge is power and ignorance is deadly. Only by understanding the offense and its capabilities will you be able to build a robust, defensive posture. Too many organizations build an ineffective security defense that does not address the true threats.3. Thinking disablement versus enablement – When an organizations' approach to security is trying to prevent employees from doing things, chances of success are much lower. However, when security is approached from an enabling perspective, it allows staff to be successful; and selling security across the organization becomes much easier. If employees are told they cannot do something (even if they do not need to do it), they will show resistance. However, if staff is informed what they can do, they are usually more enthusiastic to help.4. Not including security is part of a life-cycle – Security is not an afterthought or an add-on. It must be designed as an ongoing process. Security today does not ensure security tomorrow. Organizations are constantly changing and security must also adapt and become part of the ongoing life-cycle, not a one-time task.5. Overlooking the physical aspects of security – Buildings, rooms, data centers, physical computer access, etc. must be taken into consideration. An organization is only as strong as its weakest link. Preventing network security breaches means paying attention to the importance of strong physical and personal security.	<ol style="list-style-type: none">6. Relying on excessively weak trust or authentication mechanisms - Authentication and validation of network access is paramount. In too many organizations, authentication is the first and only line of defense. Weak authentication can easily be by-passed putting the security of the enterprise at risk.7. Failing to understand exposure to attacks on information and infrastructure – Security goes beyond having a firewall or intrusion detection systems. Security means knowing the locations of exposure points, prioritizing them and correcting them in a timely manner.8. Failing to understand and address the relationships between network, application and operating systems security – Security of each individual elements of the infrastructure does not ensure the overall security of the entire system. A comprehensive plan includes a review of all of the elements interacting with each other.9. Architecting a system that issues too many false alarms – Unfortunately, there is usually a tradeoff between false positives (system giving an alert when it should not) and false negatives (system not giving an alert when it should). False negatives represent a breach in security and most systems are designed to error on the side of the false positives. However, neither option is good and both should be reduced.10. Inadequately addressing the risk of security breaches from those within your organization – Most networks are designed to prevent attacks from occurring from the Internet. This is an important factor, but inside threats and attacks are just as critical. It is important organizations understand all potential threats and address them accordingly.
--	--