11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

Malicious Employee Attack

As companies have become more aware of the risks posed from connecting to the Internet, levels of security on these systems have greatly improved in the last few years, in response attackers have refocused their efforts on compromising corporate systems from the inside-out. This has resulted in the majority of successful attacks having an internal component to minimize the effort and to defeat the weakest link in the security chain. The fragile state of the global economy has also driven the increase in employees willing to commit fraud and perform other malicious activity. Add this to the fact that the traditional network perimeter has been extended to support remote working, mobile devices, and B2B connectivity, this has created the situation where internal threats need to be dealt with in a similar manner to how Internet based threats have been handled historically. This means taking a “data-centric” approach to IT security and applying appropriate and effective protection using methods such as access control, authorization, and encryption services.

In a 2008 Forrester Research report it was noted that the majority of security breaches involve internal employees. Numerous spectators have commented that the number of internal breaches could be as high as 85% of all IT security breaches. As a consequence, Organizations are understandably beginning to focus on how they can secure their internal infrastructure from compromise.

ASM can conduct testing to simulate real employee scenarios, such as a rogue employee in an accounts department or call center, or a disgruntled system administrator and provide insights into what information they could access and how easy it would be to remove this information from the systems in question. Whether it is from a company provided desktop or laptop, or with the aid of a blackberry or PDA, our team of consultants can test your environment for exposure and sign of compromise. ASM can run malicious employee tests that are application specific, (limited to SQL, CRM, ERP etc) or infrastructure wide. Whether it is an in depth assessment of a key application or a broader infrastructure testing program, we will look to deliver detailed and understandable reports that identify your key security weaknesses and offer useful recommendations on how to reduce the scale and likelihood of such a breach.