

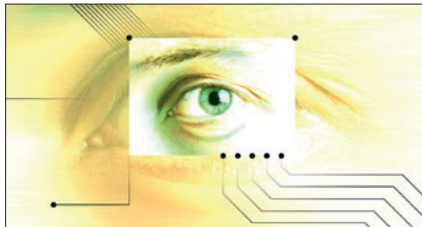


# IT Analysis

## ArcSight and Insider (or Inside?) Threat Management

Published: 10th October, 2006

**L**ook around your office. Is it full of bad people planning to destroy your organisation from the inside out? Or is it full of people doing a fair days work for a fair days pay with the usual ups and downs we all experience in life?



I would suggest that it is probably the latter, unless you happen to work for a dysfunctional organisation which, I am sad to say, do exist.

Having successfully secured the perimeters of the business world with a range of technologies, corporate IT departments are now realising that part of their threat problem actually sits inside the castle walls in the shape of the employee community.

Inside any organisation there will be disgruntled individuals and the possibility is that anyone of these could suddenly turn bad and sabotage your business. An example of this occurred at UBS PaineWebber in the US when an ex-systems administrator planted a logic bomb disrupting operations in 2002. This case finally resulted in a conviction in July 2006 and we are currently waiting for the sentencing decision due at the end of October. Rumour is it will be a long sentence.

The reason for the attack? Apparently the systems administrator was upset as his annual bonus was less than he expected.

Many other insider based security threats will go unreported as organisations try and prevent damaging news stories from emerging and damaging their reputation. Research by the Ponemon Institute reported that 78% of their 450 IT security respondents had one or more unreported insider-related security breaches. 93% cited lack of resources and 81% cited lack of accountability as primary contributing factors.

To help mitigate against the threat of insiders, companies such as ArcSight have created products to help detect and deal with such problems. The key to insider threat management, according to ArcSight, is to find the early signs of unusual behaviour, be this reconnaissance or preliminary leaks, and then respond using appropriate human resources or external legal sanctions if appropriate. By capturing a host of user and systems activity data and then applying smarts to it the team at ArcSight say they can detect abnormal behaviour and alert those that need to know quickly. An Insider Threat Package has recently been made available by ArcSight so that rules, monitoring and alerting activities can be implemented fairly quickly in a new installation.

Despite this great technology I would contend that only a very small percentage of employees are "rogue" and the vast majority are likely to become a threat out of ignorance rather than malice.

Take for example patch management. Failure for an individual to permit a patch to be installed can leave an entry point for a virus. Or loading up software from a personal USB

pen drive can introduce a Trojan. Or opening an email attachment that contains malware can quickly breach an organisation's secure boundary. Or leaving a note stuck to a PC with a user's password.

You get the idea.

Whilst products from vendors such as ArcSight have a key part to play in securing a business I would suggest that we need to use the broader term INSIDE threat management rather than INSIDER threat management when talking about security problems emanating generally from within the secure perimeter.

When considering security we all know the importance of defence in depth for building an Assured Business, as I have discussed before. We need to think through our terminology and ensure that it is appropriate and proportional otherwise we run the risk of becoming alarmist and scare mongers. This will be a huge turn off for the business and cast a bad light on all the good IT security work that is undertaken day in day out.

Inside yes, insider no.

Nigel Stanley  
*Practice Leader, Bloor Research*

© Bloor Research 2006

ArcSight, a leader in Enterprise Security Management, provides solutions that serve as the mission control center for real-time threat management, compliance reporting and automated network response. By comprehensively collecting, analyzing and managing security data, ArcSight solutions centrally manage and mitigate information risk for security, insider threat and compliance. ArcSight's customer base includes leading global enterprises, government agencies and MSSPs

published by  
**IT Analysis**

Tel (UK): +44 (0)208 123 4034 | Tel (US) +1 650-515-3474 | email: info@it-analysis.com | web: www.it-analysis.com