DEALING WITH INSIDER THREATS

BY AMOTZ BRANDES

Most people tend to neglect the need to protect themselves from insider threats.

Amotz Brandes, managing partner of Chameleon Associates, encourages more attention to be placed on preventing insider threat

Most malicious attempts on high net worth individuals begin with a leak of information from within that person's closest circles. Insider threat is usually the cheapest and most effective method for stealing sensitive information, assets and trade secrets from a person or organisation. We tend to focus efforts on IT security and invest heavily in protecting digital data. However, relatively minor attention is given to internal threats. You can build all the firewalls you want, and pay for extensive physical security measures, but these usually are not useful tools against internal threat. All efforts securing protection against IT and physical threats are rendered ineffective the moment there is a human breach.

Throughout human history we have heard stories of insider threat. Caligula famously used the Praetorian Guard to assassinate Tiberius. Insider threats – both old and common – are nonetheless too often unaddressed by the private sector. Mostly, it is government entities that do organise and maintain units devoted to countering insider threat in the public sector. But individuals and corporations unfortunately do little in the way of addressing this close and present danger.

There are good reasons why a high net worth individual or prominent corporation should protect itself from insider threat. Yet many individuals and organisations seem to feel that dealing with insider threat could potentially jeopardise personal relationships, negatively affect morale and erode trust amongst employees. This psychological barrier does differ between countries and cultures. Take as an example the use of polygraph testing to determine potential threat. In Western Europe, the use of polygraph by either government entities or by private industry is frowned upon both for legal reasons and because it goes against the cultural grain. In the U.S., polygraphs are used almost exclusively within the government and law enforcement. In Asia, Eastern Europe and Latin America, however, the use of a polygraph to deal with insider threat is far more common.

Using polygraphs to deal with insider threats

Dealing effectively with insider threat involves more than simply giving someone a technical polygraph. Instead, the organisation (that is, those professionals entrusted with conducting counter intelligence) must gain a deep knowledge of the people who work within the company. Too often, an interview is completed and although the interviewer may have a good sense of the technical qualifications of a given candidate, they still do not really know who he is. Optimally, an astute insider threat expert would conduct an applicant or employee interview with the goal of understanding: what influences this person, motivates him, makes him vulnerable? What makes him tick? A thorough familiarity with the person's character, circumstances and their psychological profile allows the security professional to accurately make recommendations to management about the degree of access, supervision and

There are good reasons why a high net worth individual or prominent corporation should protect itself from insider threat

trust which would be appropriate for that employee.

Insider threats can be difficult to prosecute. When a physical asset is involved, the path to justice is straighter than when the stolen asset is data, despite the fact that data can be all the more valuable. Although when a person steals from a governmental body, that act may well be considered treasonous, when a similar theft or breach occurs in the private sector, the act is considered unethical but is not always pursued as a criminal or even civil case.

Dealing with insider threat is not a technical process. What's more, it is difficult to arrive at absolute, evidential conclusions about a person's likelihood of becoming an insider threat. However, it is true that establishing a mechanism for dealing with this danger will reduce the potential for insider threat. It is a definite deterrent.

Detecting vulnerabilities

Often, investigation companies are asked to red team (conduct a simulated adversarial assessment) to find vulnerabilities and damaging information about a person or an organisation that could be used by the enemy. This is a service that is commonly performed specifically for ultra high net worth clients who are seeking political appointment, are moving into a higher public profile or expect to be engaging in sensitive business negotiations. The success in uncovering this information is directly connected with the ability to recruit insider sources and to conduct effective social engineering to uncover intelligence. In both these cases, investigators look for human vulnerability that is the result of ignorance, innocence or malicious intent. To close these types of gaps and vulnerabilities, high net worth individuals should educate the innocent and ignorant amongst their employees and close circles, and inform them about adversarial methods of operation and social engineering techniques.

This August, Chameleon Associates, a security consulting company headquartered in California, will be presenting a *Countering Insider Threat* seminar in Singapore. This training will teach security and intelligence, law enforcement and military professionals the principles and guidelines for establishing an effective, proactive insider threat programme.

> "INSIDER THREAT IS USUALLY THE CHEAPEST AND MOST EFFECTIVE METHOD FOR STEALING SENSITIVE INFORMATION, ASSETS AND TRADE SECRETS FROM A PERSON OR ORGANISATION."