Application of Business Intelligence & Protective Security Measures To the Financial Services Industry

Presentation to The Offshore Institute's Asia Pacific Conference, Mauritius
8th – 10th July 1999

by:

Martin E Flint

Risk Analysis (UK) Ltd
11 Waterloo Place
London SW1Y 4AU

Tel: 0171.863.8812
Fax: 0171.863.8814
E-mail: solutions@rauk.demon.co.uk

Introduction

My presentation this afternoon will aim to challenge the misconception that Business Intelligence and Protective Security Measures are normally only used by multinational corporations. Business Intelligence and Security methods, about which I will speak later, are being increasingly used by the Financial Services Community both in response to the requirement from the growing international regulatory regime, that places obligations on the Industry in member-countries to comply with the Financial Action Task Force's (FATF) Recommendations, and to meet its own internal protective security requirements.

Background

The Financial Action Task Force's key objectives, since its formation in 1989, have been to establish the measures that member countries should take in order to deter and punish money laundering, to monitor compliance, to keep abreast of the latest trends and developments in criminal activity in this area, and to encourage non-member countries to implement their Recommendations.

Money laundering can be described as any process used by criminals in their attempt to conceal the true origin and ownership of the proceeds of their criminal activity. Their objective being to hide and disguise the criminal nature of their income and wealth. The process involves placing their cash into the financial system, conducting numerous subsequent transactions to disguising the original placement, and finally using or investing the resultant "clean" money.

The UK has put in place a legal and regulatory framework which ensures that it complies with the Task Force's Recommendations and the EU Money Laundering Directive. The regime operates at three different levels, by making it an offence for any person to assist someone else to obtain, conceal or invest funds known or suspected of being the proceeds of crime, including serious tax offences. The UK Money Laundering Regulations, which came into force in 1994, require the Financial Sector to put in place systems and controls to ensure that they 'know their customers' before doing business with them, and therefore be in a position to identify transactions that appear suspicious, to keep records, and to appoint a Money Laundering Reporting Officer.

As regards the Financial Services Industry's own internal protective security requirements, these derive from its need to protect its business from dishonest individuals, unscrupulous competitors, inquisitive business analysts and intrusive media attention. As is the case with most companies, those in the Financial Services Industry will want to safeguard the confidentiality of such information as their corporate plans and marketing strategies, their personnel files and client list details.

Topics Covered by this Paper

- Due Diligence Enquiries
- Pre-Employment Vetting & Staff Security Reviews
- Executive Security Protection
- Information Security

Due Diligence Enquiries

It will be clear from my introduction remarks and background scene setting, that the requirement placed on the Financial Services Industry in member-countries to comply with all the relevant regulations is very considerable. So too is their perceived need to protect their business integrity from the various threats to which it is exposed. One of these requirements, that of knowing your customer, will be the first topic that I shall address. This requires that banks and other financial service providers to take active steps to ensure that they 'know their customers' before doing business with them. In the case of new customers this will involve asking them to complete detailed application forms, to produce documentary evidence of their identity, and quite possibly letters of introduction. It is a requirement that steps are then taken to verify the accuracy of this information. This process comes under the general heading of **Due Diligence**. For the large banks and financial service providers, serving a largely domestic market and local client base, this task has traditionally been conducted internally.

However for the smaller private banks and professional practitioners in offshore locations, serving clients who may be domiciled overseas, the increasing burden and complexity of the international regulatory regime makes the task of conducting adequate Due Diligence enquiries in a timely and cost effective manner much more difficult.

It is in these circumstances that they are increasingly turning to Business Intelligence service providers to carry out this work on their behalf. Initially the requirements were principally confined to requesting that discreet enquiries be conducted on new prospective clients from non-FATF member countries who wished to conduct very substantial business. There was also a requirement on occasion to carry out post facto due diligence enquiries on existing clients where the pattern of their financial transactions had altered significantly, and where, in the absence of any obvious explanation, this may have given rise to some reasonable suspicion.

Increasingly however the trend has been to outsource this due diligence work to specialist organisations using experienced staff skilled in investigative techniques and in the use of proprietary computer software and online databases, who can carry out this work on a contract basis, to recognised international standards, in a timely and cost effective manner.

There is also a growing realisation in the Financial Services Industry that the manner in which they may have conducted this work in the past may no longer meet present day standards, and that they should now be reviewing all their existing customer files with a view to ensuring that they comply with current regulations. This can be an onerous task for the vast majority of banks and financial service providers whose staff resources are continually under pressure, and who may not have the necessary degree of expertise to carry out this work cost effectively. One solution that the industry is turning to is to outsource this work to specialist organisations with whom they can agree on the parameters of the review and negotiate fixed fee and throughput levels. This work is normally carried out on the client's premises by a team of specialist auditors working in the evenings and weekends in order to minimise any disruption to the organisations normal routine.

The use of Business Intelligence Agencies to conduct the due diligence enquiries into new client should not be seen by the Financial Services Industry as a barrier to accepting new business, but rather as a necessary process which will enable them to take on business which they might otherwise have felt obliged to turn away. It should be seen as a safeguard, or an insurance policy, which will enable the professional practitioner to accept business with confidence in the knowledge that thorough due diligence enquiries have been completed to internationally recognised standards.

Such steps should minimise the likelihood of taking on questionable business which might attract the attention of law enforcement agencies and possibly result in a loss of reputation and good standing.

Due diligence enquiries should also be undertaken on potential business partners to ensure protection against fraudsters who are using increasingly sophisticated methods to conduct financial deception against the Financial Services Sector and their clients.

However if a situation has arisen where, through bad judgement or fraud, a professional practitioner or his client has become the victim of deception and lost funds, the application of Business Intelligence methods using their unrivalled sources and contacts in law enforcement agencies world-wide, are able to track down and locate these funds and the perpetrators. Working closely with specialist lawyers steps can then frequently be taken to recover such stolen assets.

Pre-Employment Vetting & Staff Security Reviews

The **Pre-Employment Screening** of candidates for employment in the Banking and Financial Services Industry, and of existing staff prior to their appointment to middle ranking and senior management positions has been a long established practice in many parts of the world. Here again this is a task that has traditionally been carried out within the Human Resources Departments of the organisations themselves. However with the increasing pressure to both reduce permanent staff levels and to employ temporary staff, there has been an increased tendency to contract out the task of pre-employment screening to organisations which can offer a specialist service at an agreed fee and within tight timescales.

Pre-Employment Vetting of new staff is an essential requirement in the Financial Services sector in order to establish the integrity and reliability of potential employees, and to protect and safeguard the company's assets, information, methods and business ideas.

Vetting should be conducted as a matter of course in order to reduce the risk of embezzlement or fraud by susceptible or disgruntled employees, but also to prevent infiltration by fraudsters and people with criminal records, or those potentially capable of being suborned by organised crime. In the case of cleaners and ancillary staff, the aim is to prevent out-of-hours access to your business premises by potentially unreliable persons.

Both internal and external candidates for positions within the company (including contract, temporary, and permanent staff), who may have access to sensitive or confidential information, should undergo thorough background checks. In the UK the British Standard, BS7858: 1996 Code of practice for security screening of personnel employed in a security environment, advise that that:

Screening *"should be applied equally to full-time and part-time, and to temporary and permanent employees, and to all levels of seniority, including directors. The full security screening procedure should be carried out in the case of each employee or director regardless of their previous employment, even if that employment was with another organisation engaged in security industry"*. It further advises that vetting enquiries should cover a period of 10 years.

Vetting should be an integral and continuous part of a company's security policy; however, it is often neglected until after it has become apparent that the company has become the victim of fraud.

The annual screening of employees, or prior to their promotion, should be conducted diligently. As part of the company's security procedure, staff's continued suitability for employment should become a line management responsibility. The importance of internal controls at all levels of management is essential so that the company may be made aware at the earliest opportunity of any changes which may indicate that an employee's suitability might have become questionable.

Application forms and vetting procedures for new employees should be designed to obtain the maximum information about an individual in order to conduct thorough background enquiries.

In the case of cleaning and ancillary staff employed by outside contractors, part of the contract with such firms should make vetting compulsory by the provider. Such staff should only be allowed limited or supervised access to sensitive areas.

Contracts of Employment should contain a confidentiality clause so as to prevent potentially valuable information leaving the company with an ex-employee.

Key Executive Security Protection

Introduction

Risks in varying forms and degrees are an inescapable feature of daily life. For individuals living and working a normal civilised existence there can be no possibility of creating a totally secure environment. However in order to assess the particular security risks to a company's Key Executives, and to manage them to an acceptable level, it is necessary to review the security environment in which they live. The introduction of formal Risk Management methodology into the security field provides a sensible and balanced means of determining the appropriate levels of security for different sets of circumstances – and thus avoiding overly extensive and rigorous security measures which can be intrusive, inconvenient and costly. Risk Management can be described as the organised process of managing uncertainty.

The UK Security Environment

The UK mainland enjoys political and economic stability. Nevertheless a range of threats does exist which place at some risk the safety of Key Executives, the security of property, and the disruption of normal business activity. Principal among these is the threats from terrorism, criminal activity, business espionage and media intrusion.

Terrorism

It is a characteristic of terrorism that it occurs when least expected against targets least prepared for it. While the threat from Irish terrorism is currently greatly reduced, there is a large Middle Eastern community in the UK which has lead to a certain amount of terrorism in the UK. The greatest current uncertainty lies with the potentially violent response to the bombing by the US in August 1998 of Islamic Extremist terrorist targets in Afghanistan and Sudan, the continued bombing by US and UK of Iraq, and in the aftermath of the civil war and ethnic cleansing in the former Yugoslavia. Other local factors including armed conflicts will present varying degrees of threat elsewhere in the world.

Overall the threat from terrorism on the British mainland generally is currently assessed as Low to Moderate, depending upon individual circumstances – though this can of course change at any time.

Animal Rights Extremists

A large number of explosive and arson attacks continue to be mounted by extremist members of "Animal Rights" groups, who were responsible for some 800 incidents in 1997, causing nearly £2 million worth of damage. For institutions and individuals connected with the use of animals for research, the threat remains Moderate to High.

Politically Motivated Violence

The threat of politically motivated violence and sabotage on the British mainland is generally Low, however there are a small number of extremist pressure groups which will exploit opportunities for disruptive action to embarrass the authorities and large corporate bodies.

Burglary and Car Crime

The threat from crime in England and Wales varies according to age, sex, location and social category. Burglary and attempted burglary was inflicted upon 5.6% of all UK households in 1997. The highest risk is in low-income inner-city housing areas and certain urban districts of high-income residents. However, targeted burglary in the more prosperous areas by skilled criminals is no respecter of statistics.

The majority of vehicle crime involves the theft of the contents, putting at potential risk confidential papers and electronic media containing sensitive company information.

Kidnapping

Incidents of conventional kidnapping for ransom, and 'tiger' kidnapping - which involves the taking and holding of a hostage with the intention of forcing that individual to assist in the immediate theft of money or property from their employer - are fortunately rare in the UK. There were only twelve such incidents recorded between January and October 1998.

Blackmail & Extortion

Experience of known blackmail cases in the UK has shown this to be mainly an opportunist offence against homosexuals, convicted paedophiles and adulterous individuals. There have however been a growing number of extortion threats and actions to contaminate products or to disrupt businesses with bomb alerts. By October 1998 the number of reported incidents had exceeded the 40 such cases during 1997.

Business Espionage

There is a good deal of unpublished evidence to show that business espionage (involving the undetected theft of confidential information), is widespread throughout all industrialised countries. Telephone interception and electronic eavesdropping (bugging) are targeted against key people and sensitive meetings. Private investigators are often employed to use their particular skills and resources. Sensitive information

about an organisation is extracted to harmful effect principally by its own or contracted staff.

Media Intrusion into Personal Privacy

There is no statute in the UK which protects privacy. Even the Broadcasting Act 1996, which directs the Broadcasting Standards Commission to manage a voluntary code of practice aimed at avoiding unwarranted infringements of privacy by programme makers, contains no definition of privacy. Respect for privacy and avoidance of harassment by printed media is also self-regulating, administered by The Press Complaints Commission. This body has the dual function of protecting the rights of the individual and upholding "the public's right to know". The disruptive effect of media intrusion against Chief Executives and high profile individuals, and their immediate families, can be traumatic.

International Travel

All the threats referred to above apply in varying degrees in different countries throughout the world, in some cases with higher levels of uncertainty. A criminal organisation's perception of large multinational corporations is that they have ready access to large sums of money with kidnap insurance for their Key Executives.

The threat against Western tourists and businessmen from terrorism and hostage taking in many developing countries has increased in recent years. Wherever uncertainty exists Key Executives should seek advice and individual country assessments before travelling.

Measuring and Monitoring the Security Threat

Threat is defined as a source of potential harm, or a circumstance which could cause injury, loss or damage. The threat from criminal activities, business espionage and media intrusion, is substantially higher for individuals with a high public profile, substantial wealth, influence and responsibility. Security planning therefore needs to allow for an immediate tightening of security procedures in response to any increase in the levels of threat.

Consideration should also be given to the detrimental consequences to an organisation in terms of the effect on corporate management, financial confidence in the market place, and on the disruption to business that would arise from any successful 'attack' on the company or its Key Executives. It is well recognised that the underlying circumstances behind a major security incident affecting the safety of Key Executives or any member of their immediate families, could have unforeseen, far-reaching and highly distressing personal consequences. Depending on the seriousness of the incident, intrusive media attention could also be extreme and lasting, and likely to result in severe disruption to business operations generally.

It therefore cannot be emphasised too strongly that large corporations have a duty of care to their Key Executives to review the level of threat to which they are exposed by virtue of the positions they hold. This responsibility requires that a thorough personal security review be undertaken, and that recommendations to reduce vulnerabilities

and for efficient arrangements for monitoring the threat should be implemented. Any indications of potential trouble should be reported immediately, the level of threat reviewed, and the security procedures strengthened as necessary.

Security Surveys of Home Addresses

An essential element in assessing the vulnerability of Key Executives to a variety of security threats is the undertaking of thorough surveys of their home addresses, leading to recommendations aimed at reducing any vulnerabilities.

Security surveys involve a physical inspection of the house and grounds, as well as the immediate local environment, in order to establish the presence and effectiveness of existing access controls and emergency communications. The security of external and internal door and window locks is inspected, as is the effectiveness of intruder alarm systems and the response to their activation. Storage arrangements for sensitive working papers, vehicle parking and security arrangements, and all external security lighting are examined. Details are sought about the composition and lifestyle of the Key Executives' immediate family, the presence of valuable contents in the home, as well as procedures for dealing with callers to the house and on the telephone. Arrangements for the vetting of drivers, gardeners and domestic staff are examined, as is the professional competence of the driver for dealing with potential security incidents. Contact is also subsequently made with the local police and the domestic insurance industry to seek details of the prevalence of burglary, theft and other related crime in the area.

Report and Recommendations

On completion of the detailed security review, an individual risk assessment is prepared taking into account all the circumstances unique to the company and its Key Executives. The report also contains a section detailing the results of the survey carried out at the Executive's home address, and incorporating the findings and photographs, together with specific recommendations to substantially reduce all identified security vulnerabilities.

Information Security

The Financial Services Industry has long been aware of the need to safeguard its confidential and sensitive information. Nevertheless this is a very specialist field and it is for this reason that the banks and financial service providers have traditionally employed specialist staff with appropriate first-hand experience, and outside consultants to assist them in this task.

It is fundamentally important that adequate protect security measures are put in place to protect the company's information, and that these are regularly reviewed. The organisation should aim to ensure that there is a greater appreciation by all its staff of the range of insidious threats to which its sensitive information is exposed, and the steps that can be taken to implement effective measures to protect it. We are all well aware that organisations possess sensitive information and data which if lost or stolen, or if it fell into the wrong hands, would adversely effect its business.

The first step that any organisation should take is to identify that information, among the mass of data held by it, which to a greater or lesser extent is sensitive. This can be defined as data which if it became known to information brokers, competitors, institutional investors, the media, radical group or the general public, could have seriously adverse consequences.

We have already touched on some examples of the type of information that requires protection, e.g. corporate plans and strategies, financial information, customer and client lists, research and development plans, marketing strategies, plans for mergers, acquisitions and take-overs, information about bids and tenders, proposals for plant or office closures and staff redundancies, personnel files, contributions to political parties, capital investment plans, new products and services etc.

We also need to consider very carefully, preferably with the assistance of the organisation's professional security advisers, which outside persons or organisations represent a threat to your sensitive information. Such a list might include information brokers, unscrupulous competitors, the media, single-issue group, investigative journalists etc.

Bringing these two strands together should enable us to determine what information needs to be safeguarded and from whom, and therefore the degree of protection that is commensurate with the threat and the likely cost of exposure. This threat assessment enables us to devise and adopt an appropriate and coherent series of protective security measures.

All organisations posses information which they need to safeguard. What are the aspects that need to be considered when planning how to go about doing this?

Formulation of Corporate Security Policy

The organisation needs to designate a Main Board Director responsible for all aspects of corporate security. His duties should include chairing a committee on security involving all relevant senior departmental managers covering such functions as R&D, Human Resources, Finance Department, Auditing, IT, Facilities, Administration, Production and Purchasing. They should determine the type of information that the company needs to regard as sensitive and requires protecting. The Security Committee will need to determine who should be responsible for classifying sensitive information, how it will be stored, and the procedures for its secure handling, copying and destruction. Consideration will also need to be given, as we have discussed earlier, to the vetting of employees and contractors who will have access to such information. Once all these aspects have been thoroughly considered, they need to be formalised into a Corporate Security Policy and Procedures Manual.

This document, which will vary considerably in length from one organisation to another, should be reviewed annually to ensure that it continues to meet the requirements of the organisation, and that any procedural deficiencies which are exposed are addressed. Staff and contractors with regular access to sensitive information should be required to sign the document annually to confirm that they are aware of and follow the company's security procedures. The document should also

lay down disciplinary procedures and sanctions. Managers should be notified of lapses and be held ultimately accountable for implementation of security procedures, and the actions of staff in their departments.

Formulation of Corporate Contingency Plans

The organisation's contingency plans to deal with major security lapses should be considered, formulated, and incorporated in the company's business recovery programme. These should cover all forms of foreseeable disasters such as fire, product contamination, theft of computer microchips etc. Details of the staff who will compose the company's Response Team should be assembled so as to ensure that the relevant personnel can be quickly contacted and, if necessary, assembled in the event of an incident arising. It may also on occasion be necessary to bring in outside parties such as advertising agents, PR consultants, legal advisers and insurance brokers to deal with some particular problem. It is preferable to consider and decide upon the composition of such a group before an emergency arises, and to have all their relevant office, home and mobile telephone numbers readily to hand.

Conclusion

As I stated at the outset the aim of this presentation was to challenge the misconception that Business intelligence and Protective Security Measures are only used by large multinationals, and to demonstrate why such measures are being increasingly used by the Financial Services Industry – driven largely by the growing demands of the international regulatory regime, and to meet its own internal protective security requirements in an increasingly hostile business environment.