

Keeping One Step Ahead in 2009

Threat Assessment

Author:

David Carrick

Date

December 2009

KEEPING ONE STEP AHEAD OF NEW THREATS IN 2009

David Carrick, CEO of Memex

For many global and multi-national organisations, this year represents an ideal opportunity to examine and improve threat management strategies. Year on year, threats in the areas of terrorism, organised crime and commercial crime are becoming increasingly sophisticated and complex and are spiralling in scale. For decades, heads of risk, heads of fraud and information intelligence chiefs within global and multi-national organisations have been well-versed in the basics: How to respond to and protect their organisations from terrorism, organised crime, and fraud.

However, the current economic downturn, predicted to continue for the next three years, is proving to be a fertile breeding ground for these types of threats. Existing threat management strategies may require more than a simple “spring clean” and a rigorously up-to-date approach may be required. While it can certainly be argued that 2009 holds some potentially daunting prospects, I strongly believe that, armed with the right threat management software solution, organisations, business and law enforcement can remain one step ahead of the criminals. In this article I will examine the threats and talk about how the right software can help tackle the issues.

The Threats: Terrorism

Before 9/11 occurred, terrorism in the UK was usually linked to organisations such as the IRA, and was primarily dealt with by top level Government agencies and specialist police units. The comparatively small pool of information required meant that sharing of information was much tighter and therefore easier to manage. But now, the unpredictable and volatile nature of modern terrorism means information is required from sources rarely used in the past to identify the link in an investigation and to identify developing threats. This has created an imperative need for both improved collection and a national information sharing network in the UK. When investigating or identifying terrorism plots it is often the tiny but vital piece of information that completes the jigsaw so partnership information – the data that is shared between police forces and local authorities for example – has become extremely important.

The Threats: Organised Crime

Tackling terrorism is high on the national agenda – and rightly so – but as a result police forces are increasingly over-stretched, and dealing with business related crimes is viewed as a lower priority in comparison to national security. However, organised crime

and fraud networks are becoming increasingly sophisticated, operating like multinational companies. To a degree their growth relies upon a lack of partnership between Government, law enforcement and business. Several factors are exacerbating this situation. The downside of the Internet revolution is an increasingly significant risk. Its widespread adoption into the lives of consumers and business is proving a powerful lure for organised gangs, who follow money by moving on-line with their criminal activity. And when Internet misuse combines with the opening of country borders, it makes for a dangerous blend, creating “grey markets”, which move rapidly from country to country, threatening to erode revenues, contaminate supply chains and dilute brands.

Globalisation is also an escalating trend in 2009. Like Internet technology, many positive aspects are accompanied by significant threat, particularly increased opportunities for counterfeiters, parallel traders and anti-corporate extremists. And of course the continuation of 2008’s economic downturn brings a potential surge of serious, organised crime and black market growth.

The Threats: Commercial Crime

Traditional white-collar crime is experiencing a dramatic upsurge. One of the effects of the recession is the dramatic negative impact on middle class lifestyles.

Correspondingly, financial fraud is on the increase, with potentially more incidences of false insurance claims and credit card fraud. These types of threat have always existed, but continue to evolve, hand-in-hand with the growing economic crisis.

Business needs to examine more closely than ever potential internal threats from white collar staff. There is a sense among some financial institutions that the behaviour of certain traders intensified the current financial situation. A whistle-blowing procedure could have lessened, and perhaps even helped avoid, the effects of recession. I believe that in the current economic climate, business should be looking at significantly improving their whistle-blowing procedures and solutions.

Threat management solution

Compared to the smaller, lower-tech threats of, say, twenty years ago, the increasing scale and complexity of the threats I have outlined can seem overwhelming. But the right threat management solution can offset threats before they truly take hold.

The information management software used successfully within law enforcement transfers very favourably as a robust threat management solution for the business world where the ability to gather, store and analyse intelligence from multiple sources at speed is also required. But just as in a law enforcement environment, to be truly effective the right threat management solution must form the information management backbone of an organisation’s diverse intelligence tools, procedures and programmes. It has to support the understanding of complex threats by other measures such as intelligence monitoring and vulnerability assessments. In short, the right system provides actionable, key and timely data for principal decision makers.

For example, when it comes to external threat in the commercial arena, it’s important that information management software enables financial services companies to

proactively target individuals and gangs attempting to de-fraud their business. This will allow them to predict and prevent losses before they would otherwise occur, and to respond coherently to emerging threats.

The correct procedures coupled with the right software solutions can give staff the confidence to report on internal fraud. In a recent survey by KPMG, it was found that one of the best tools against financial crime is internal reporting of suspicious activity. In addition to specialist technologies that can detect anomalous transactional or staff behaviour, the right threat management solution must also offer a secure and legislative-compliant mechanism for both the internal and external reporting of suspicious activity. This allows businesses to harness the power of their own staff in the fight against internal fraud.

The benefits

Any modern threat management solution should be based upon an intelligence engine that reveals hidden links and relationships between entities across any number of disparate systems. Main examples would include watch-lists, Suspicious Activity Reports, covert sources, industry emails, intelligence report archive and websites. Information from these disparate systems is drawn into one central repository, allowing investigators to analyse information in real time, and generate hard, actionable intelligence, within a secure, managed environment that guarantees regulatory and legislative compliance.

There are a number of benefits to be realised by deploying this type of solution. By linking multiple systems, each holding small pieces of a very complex criminal jigsaw, businesses can identify and take the necessary steps to reduce fraudulent activity. By delivering a common intelligence platform, an organisation can create its own “crime IQ”. Basically, fraud and risk managers gain what can be described as a “dashboard view” not only of threats, but also of their team’s activities in response to identified areas of concern, such as repeat insurance claims from the same source. Ultimately the right solution allows decision makers to respond based upon the widest pool of information available.

For example, an effective threat management solution screens insurance claims with the aim of increasing recovery rates. This technology creates rules or red flags, against which claims can be screened and scored as part of an automated process. An obvious example might be multiple claims from one person using different aliases. A more complex example might be where both parties involved in a car accident employ the services of the same lawyer, doctor or car repair shop. In other words the system detects the known or suspected *modus operandi* of individual fraudsters and complex fraud rings.

Financial services companies using this kind of system have seen a 30% uplift in the number of claims being referred for investigation, and an increase in recovery rates from the industry standard of 10% to 42%. Suspicious claims that slip through the net either due to operator error or training issues, or simple inability to spot fraud are automatically forwarded to a financial services Special Investigations Unit. Financial services

organisations are already relying on this style of threat management solution to consolidate large amounts of information and intelligence-related data from multiple public sources, and to provide their analysts with advanced analytical tools and techniques to develop their actionable data further.

The growth in efficiency is similarly impressive. Before the introduction of this style of solution, claims were referred for investigation manually by claims handlers, so in addition to the uplift in referrals, the solution saves claims handlers a significant amount of time and improves the effectiveness and efficiency of claims handlers.

Staying one step ahead of the criminals

In order for businesses to effectively and efficiently tackle crime, especially in the current economic climate and in light of the emerging new threats outlined, it is vital to take a similar approach to law enforcement and implement a robust threat management software solution.

Of course, the type of threat faced by business will continually evolve so it's equally vital, again just like law enforcement, that the threat management solution is flexible allowing for almost any eventuality. Indeed the capabilities of the right system need to continually expand in line with an ever changing threat environment, providing organisations with better indications and warnings of threats.

My advice is for business in 2009 is to tackle the threats head-on, be proactive in improving your risk management strategies and reap the rewards of becoming truly "intelligence-led" with the right threat management solution in place.

David Carrick is the Chief Executive Officer of multi-national information management software experts Memex. Based in East Kilbride, Scotland, he is a board member of the Scottish North American Business Council. Memex software solutions are deployed globally by a diverse range of organisations, across law enforcement, government and commercial sectors, helping them to predict, prevent and respond to threats in real time.

Contact Us

Memex Technologies Ltd and Memex, Inc

UK and International

Memex Technology Ltd
2 Redwood Court
Peel Park
East Kilbride G74 5PF
Scotland
Telephone: +44 (0)1355 233804
Fax: +44 (0)1355 239676

America

Memex, Inc.
22636 Davis Drive, Suite 130
Sterling, VA 20164, USA
Telephone: +1 703 556 4031
Toll Free: +1 866 MEMEXUS
Fax: +1 703 556 4282

Copyright ©

No part of the contents of this publication may be reproduced or transmitted in any form or by any means without the written permission of Memex.

More Information

For the latest information about our product and services, please visit

<http://www.memex.com>