sponsored survey analysis

Financial crime survey 2013

Since 2007, *Operational Risk & Regulation*, in collaboration with **BAE Systems Detica**, has conducted an annual survey covering key industry trends in financial crime, risk and compliance. The 2013 survey results show continuing recovery and strengthening of investment in operational risk, anti-fraud and compliance solutions. However, the focus and priorities of financial institutions continue to change in line with both service evolution and technological innovation

A key litmus test of the overall health of the market is the general and expected movement of financial crime budgets. Over the last six years we have seen sustained growth in investment despite retrenchment and cutbacks elsewhere in financial services, and this year's survey again shows expected growth into 2014.

While just under half of all respondents indicated that budgets will be broadly the same in 2014, an average 45% of respondents by segment indicated that they expected budgets to grow by up to 20% across anti-money laundering (AML), fraud and tax compliance. An interesting outcome is that 8.5% of respondents indicated they expected the budget allocated to meet the requirements of the Foreign Account Tax Compliance Act (Fatca) would grow by more than 20% in the coming year (see figure 1).

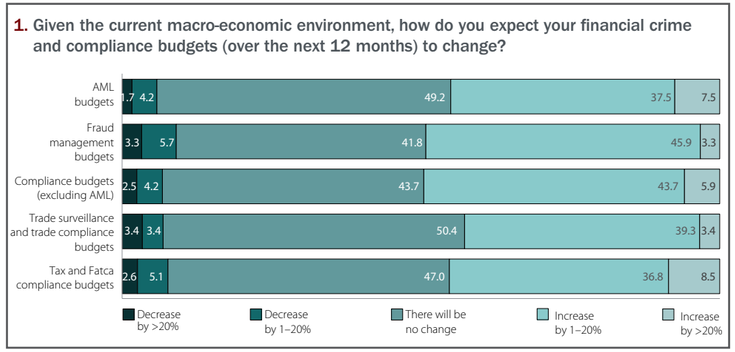
It is worth noting that between 4% and 9% of respondents indicated they expect financial crime budgets to decrease in some areas in 2014. While this is noticeably higher than in 2012, it is in line with 2011 and previous years.

We asked respondents what the financial crime priorities for senior management would be in the coming year. While there is a diverse set of respondents across all areas of financial crime and priorities will vary based on lines of business, the high-level trend is in keeping with 2012, with a few notable changes (see figure 2).

Respondents indicated that the focus on cybercrime and the related areas of online and payment fraud remain the overriding priorities for senior management for 2014, although the lead is down marginally on 2012. It is unsurprising that cybercrime remains the key priority area in 2013.

Apart from the headline-grabbing focus on mass compromise incidents at Adobe, Sony and Citigroup, to name but a few, there have been many less high-profile breaches of both personally identifiable information and commercially identifiable information at financial institutions and data suppliers over the past year.

1. Given the current macro-economic environment, how do you expect your financial crime and compliance budgets (over the next 12 months) to change?



In the most recent BAE Systems Detica Cyber Security Monitor research, carried out by Ipsos Mori, 73% of respondents perceived the most likely group to mount targeted attacks are professional fraudsters – by far the most frequently mentioned group. A majority (86%) of the companies polled who had estimated the potential damage of a successful cyber attack estimate impacts at the level of tens of millions of pounds. One-third (34%) of those respondents thought it would cost more than £50 million. None believed damage would be less than £1 million. The research was carried out among senior business and IT decision-makers working in UK companies with turnovers in excess of £350 million.

A defensive chain in financial crime prevention is only as strong as its weakest link and, increasingly, that link lies in the hands of the end-user. The susceptibility of mobile devices in the workplace to hacking and data monitoring continues to be a serious concern, particularly in a financial services environment increasingly mediated by electronic devices externally and 'bring your own device' internally.

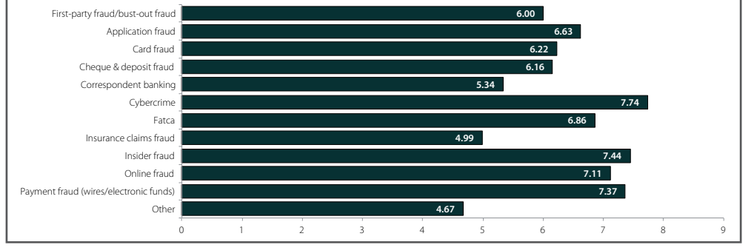
Well-publicised threats from malware, Trojan horses and botnets tend to be widely reported. Other threats to organisations and their customers from lost or stolen devices, insecure communications and mobile applications are often less prominent, though equally concerning. It is against this backdrop that the US, UK and European authorities are seeking not just to extend data-breach recording as a statutory requirement, but also to impose a regulatory obligation to have financial and cybercrime defences within systems operations ahead of a service or product launch and in advance of any potential commercial loss.

The biggest changes observed in 2013 relate to the increased focus on insider fraud and, perhaps more surprisingly, Fatca in the US. These have risen substantially in priority for senior management, as both issues have increased considerably since 2012. Fatca was originally believed to be focused around private banking and corporate banking, particularly within tax havens, but the regulations have evolved, bringing a wider set of depository, cash-value insurance products and custodial financial accounts into scope, meaning Fatca has a much wider impact across financial services. Many countries with major financial centres have entered into Fatca-style agreements with the US to ease the burden on their financial sectors. This means that financial institutions in those centres will have obligations to their domestic tax authority. This increases the impact of Fatca and merits greater attention from senior management.

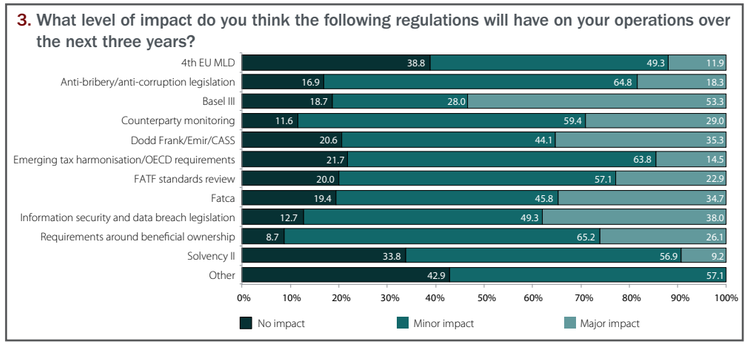
It is notable that the most recent Financial Action Task Force (FATF) guidance to national governments seeks to make tax evasion a predicate offence. The European Union (EU) G5 announcement in April on information sharing, the G8 Lough Erne Declaration in June and announcements between the UK government and Crown Dependencies and Overseas Territories to improve international tax compliance all suggest this is a long-term programme that will extend far beyond US tax and, which, at the time of writing, are due to come into effect in July 2014.

We next asked respondents which of the current regulatory themes they expected to have an impact on their operations in the next three years.

2. What types of financial crime initiative are currently a priority for your senior management team?



3. What level of impact do you think the following regulations will have on your operations over the next three years?



The respondents indicated overwhelmingly that Basel III will have a major impact over the next three years, which is likely to continue through the transitional period to 2019. This is the largest 'major' impact ever recorded in our survey. Basel III is challenging financial institutions to change business models to enhance supervisory and fiduciary oversight to improve the quality of capital and contain potential economic mishap.

The focus on capital and liquidity reform is leading to comprehensive reappraisals of risk-weighted assets and systemic risks and interconnections throughout the financial ecosystem. This is clearly presenting organisations with many challenges that will continue long into the foreseeable future.

The focus on stress testing is giving rise to implementation challenges. As the scope of Basel III spans such a wide spectrum of operational risk and financial risk management, it is easy to understand why it is perceived as a key regulatory theme (see figure 3).

Another area identified by respondents as having a 'major' impact over the next three years is that of information security and data-breach legislation, of which we have seen many examples over the past year.

While data-breach notification has been enacted in US states since 2002, EU data-breach regulations came into effect in August 2013, mandating data-breach disclosures for telecoms operators and internet service providers for theft, loss or unauthorised access of data, including emails, internet protocol and call data within 24 hours of the service provider becoming aware of a breach. This is widely believed to be a precursor to a more expansive protection framework with a wider application within financial services as set out in the proposal for the protection of individuals for the processing of personal data and the free movement of such data (General Data Protection Regulation).

One final trend that appears to be universal among respondents is how new financial crime problems and solutions are addressed in a variety of ways as they emerge over time. During the six years we have conducted the survey, we have seen a consistent trend with regard to financial crime solutions. They are initially addressed using a variety of internal and external approaches but, as changing requirements have placed a continuing burden on financial institutions, there is a consistent year-on-year trend to migrate to or reinforce defences with onsite vendor solutions or hosted solutions.

In summary, this year's research has once again provided deep insight into the key trends and the state of the market. Investment in financial crime defences is increasing for between 40% and 50% of respondents. The focus on cybercrime continues to be the leading trend as we enter 2014, but other areas of focus such as Basel III, insider fraud and new requirements in tax disclosure and reporting have also increased in prominence throughout the year. *www.deticanetreveal.com*