StrategicRISK

RISK INNOVATION

SHOWCASING RISK MANAGEMENT MATURITY AROUND EUROPE

November 2014

Financial institutions

IN ASSOCIATION WITH

ZURICH®

INTRODUCTION

The seven-year (and counting) hitch

When it comes to risk, the effects of the 2007-08 crisis are still being felt today. So, where do financial institutions go from here?

Financial institutions are the cornerstone of the global economy, but they are also exposed to an ever-increasing range of risks. From economic turbulence to geopolitical unrest, cyber threats to regulatory scrutiny, these organisations operate in a world of rapidly changing and sometimes conflicting pressures as never before.

The fallout from the financial crisis that began seven years ago has seen regulators take a tougher stance and financial institutions revert to a more introspective view of their operations, as Tim Atkin, Zurich Global Corporate head of customer, distribution and marketing EMEA, reminded delegates at the Financial Institutions Risk Forum co-hosted by *StrategicRISK* and Zurich in October 2014.

Basel III is perhaps the most visible regulatory reform to result from the financial crisis and is unlikely to be the last, according to Steven Hall, a partner in financial risk management at KPMG Risk Consulting and a keynote speaker at the forum (pp12-13). He challenged delegates to consider the likelihood of a Basel IV.

Connected to the speedy regulatory reform are restrictions aimed at limiting potentially dangerous activity by employees of financial institutions. It is almost 20 years since Nick Leeson's trading losses brought down Barings Bank and, in a keynote speech (pp8-9), Leeson identified a failure to ask intelligent questions as a consistent flaw within financial institutions that enabled him – and many more since – to inflict so much damage.

Looking beyond the regulatory framework – and its issues connected to cyber and technology, which provide some of the most vexing challenges for financial institutions – delegates were able to flesh out their digital demons in a risk clinic hosted by BAE Systems director of cyber services James Hatch.

This was followed by the final keynote speech of the day, by EY's assistant director of fraud investigation and dispute services, Massimo Cotrozzi: see pp10-11.

The forum closed with an illuminating panel debate moderated by Luca Ravazzolo, global financial institutions lead in global underwriting at Zurich.

The panellists included three senior representatives from Zurich and two risk managers from high-profile European banks.

The true cost of reform

Ravazzolo began by asking panellists for their thoughts on regulatory changes. One of the panellists pointed to the increased significance of risk management at board level as a result of these reforms and also highlighted the cost.

"Risk is now at the highest point of the board agenda. It also means we are spending a phenomenal sum of money only to keep pace with the changes, and that doesn't include things around financial crime and money laundering, for example," a panellist said.

Another participant agreed: "Risk management has moved higher up the 'pyramid priority' within my organisation. There are now more opportunities for risk managers to become involved in senior management meetings. This is positive and helps to increase interaction with other areas within the business."

With regard to regulatory changes, one of the Zurich representatives identified three sets of challenges facing banks and insurers.

They said: "One group is macro-prudential and micro-prudential, which includes legislation such as Solvency II and Basel III. The second is regarding consumer protection... and lastly, delivering multinational insurance programmes in a compliant way represents a challenge for global insurers in a fragmented regulatory landscape."

With the discussion moving on to claims services, one participant underlined the size of the challenge facing insurers following the financial crisis of 2007-08.

One panellist said: "We recently paid off the direct claims from the subprime crisis and are now in the process of paying indirect ones, which include D&O-related issues. "Now we are getting into the third wave of claims, which are around conduct issues."

Shutterstock

When the debate moved on to product innovation, one risk manager raised concerns about the insurance industry's ability to address the needs of larger institutions.

Another participant highlighted the importance of holding conferences such as this one for insurers to offer an opportunity to listen to the needs of their clients and added that Zurich was already working towards improving its product range.

They said: "There is a point to be made for the larger organisations that have unique exposures, and that is where the customised solutions can be important."

The issues discussed at the forum are explored throughout this supplement.

A breakdown of responses to the survey, in which risk professionals gave their thoughts on the main challenges facing financial institutions, can be found overleaf. **SR**

THOUGHT LEADERSHIP

LUCA RAVAZZOLO
Global financial institutions lead, Global Underwriting, Zurich General Insurance

AN INTERCONNECTED WORLD

The survey confirms that threats facing financial institutions (FIs) are interconnected. If we look at the top five risks the respondents identified (changes to regulation; cyber risk; technology/system failure; reputational damage; economic slowdown), it is clear the risk of reputational damage underpins most of these top concerns.

The pace of regulatory change poses compliance challenges and, if laws are flaunted, FIs will suffer reputational damage. If a bank's reputation is tarnished, its revenues will drop and its top line figures plummet, but other banks' financial fundaments will also be affected.

Seventy percent of respondents considered brand damage as the most difficult risk to insure. Currently, there is no way to quantify the immediate loss arising from brand damage. This makes it hard to create insurance for this risk, as the loss can be assessed only months after an incident has happened. Further, reputational damage may arise from many sources.

However, several solutions indirectly cover the consequences of the threat, for example. D&O insurance. If FIs struggle financially or the share price significantly drops, and investors and shareholders want to take action against the company, D&O insurance can provide indemnity to the bank and its directors as an immediate solution to cover costs and expense and any potential liability.

FIs can do more to mitigate the effect of this threat by taking action following an incident through communication campaigns. This is vital, particularly for the next wave of banking scandal: manipulation of the Forex market. Analysts estimate these incidents could cost billions in damages, fines and penalties.

Guilty banks cannot mitigate their past actions. However, they have made provisions for litigation. They cannot avoid the potential reputational damage, but how can they better manage it? The key is through transparency and public communication and demonstrating that the rest of the business is in order or that the problems that gave rise to a past misconduct have been identified and corrected.

The most concerning element of the survey is that risk managers think insurance is becoming more a commodity and is no longer an effective risk management tool. One respondent said that, in the past, brokers and insurers were seen as key partners as they provided the insurance solutions to meet their evolving risk transfer needs. Now, 70% of respondents consider a lot of their risks uninsurable.

This view needs to change and communication between risk managers and insurers needs to improve. Otherwise, we create a barrier no one wants.

SURVEY RESULTS

Behind the numbers

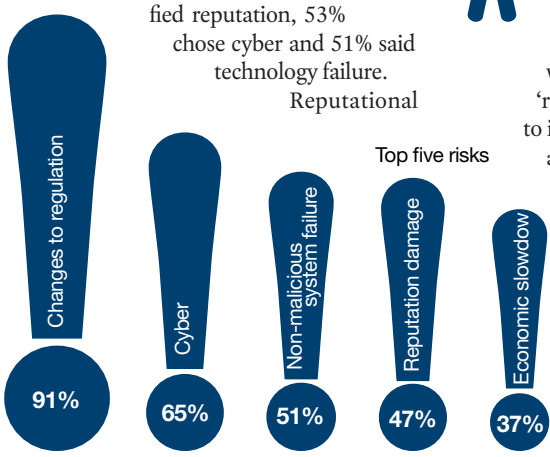
A survey of senior risk managers in the financial sector reveals a complex landscape of interlocking risks, with regulatory change and cyber risks coming top of the five main risks. The survey also shows how the financial crisis affected the way in which the risk management function is perceived in financial institutions

StrategicRISK surveyed the most senior risk professionals at financial institutions, including investment banks, insurance companies and retail banks in Europe's biggest economies to understand the key issues facing the financial sector. The findings reflect a complex risk landscape, with most of the top five risks interlinking with one another, increasing risk exposure and potential losses.

Respondents said the following threats are among their top five risks: changes to regulation (91%), cyber risk (65%), non-malicious system failure (51%), reputation damage (47%) and economic slowdown/stalling recovery (37%). In a risk landscape where these threats are interconnected, the potential loss for a company will be significant.

Further, the insurance market is failing to address many of these key risks according to the survey.

When asked to list the hardest or impossible risks to insure, 70% identified reputation, 53% chose cyber and 51% said technology failure.



Reputational damage, for example, can be linked to cyber risk and non-malicious system failure. Data breaches and system failures could lower public confidence, particularly when personal finances and private information are at stake, as was the case with the US department store Target. In 2013, the company suffered a security breach in which hackers accessed personal information of about 70 million customers. The cost associated with the breach amounted to millions of dollars.

Regulation

Indeed, the regulatory environment is becoming stricter on areas such as financial reporting or data protection. Regulations that aim to protect personal data increase the compliance burden for companies and their breach can potentially lead to fines and reputational damage.

Regulation was also cited as an area lacking in insurance cover. Although 'regulation' was not offered as a choice in the multiple selection part of the survey, when asked to specify the most difficult risks to insure, respondents alluded to it in some shape or form.

One respondent said regulatory change was an uninsurable risk, while others stated 'regulations' or 'regulatory impact' were difficult areas to insure. This, coupled with the fact that an overwhelming 91% of risk managers said regulatory change was one of five top risks, illustrates a landscape where risk managers are struggling with the regulatory environment.

Interestingly, risk managers feel their role is driven primarily by regulatory changes. More than 80% of respondents said risk management practices in the industry are improving, with 58% citing regulation as the primary driver of those improvements.

As one respondent put it: "[Risk] practices are improving only through changes in regulatory requirements. I am not sure if this means that risk management is embraced or if it is merely done to comply."

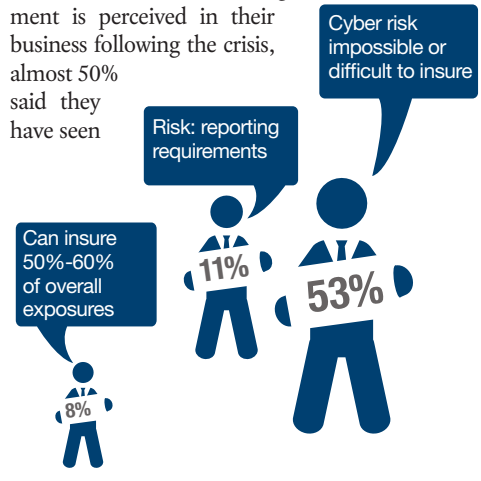
However, one risk manager viewed it differently: "Regulators are enforcing fast change in the compliance and risk control area, withholding the development of risk management."

Other respondents, on the other hand, thought the improvements in risk management were due to advancements in technology and greater communication between risk managers and the board.

Financial crisis

The survey also reviewed how the economic crisis has affected how risk management is perceived in the respondents' companies. More than 50% of respondents believe their organisation has become more risk-averse, compared to a smaller proportion (16%) admitting that their company had not made any risk management improvements and a further 28% said there has been no change since the financial crisis.

In terms of how risk management is perceived in their business following the crisis, almost 50% said they have seen



no change, compared to one-third who believe the crisis has improved the importance of risk management.

Risk transfer

Although all respondents use risk transfer solutions, they identified gaps in the insurance market, including costs arising from human errors, liquidity, supply chain and, to a lesser extent, credit risk and natural catastrophes.

In addition, 40% of risk managers said the percentage of insurable risk represents between 20%-30% of their firms' overall risk exposures. A further 19% of risk managers said between 30%-40% of their risks were insurable and 2% are able to transfer 60%-70% of their firms' risks through the insurance market.

The relationship between insurance and client is an area that needs to improve, according to the survey. When asked 'how can insurers better assist you in the identification, management and transfer of risk?', many answered that the relationship between insurer and client must be strengthened, with suggestions of more frequent meetings and regular communication.

The fact that three of the five top risks from the survey (cyber, non-malicious system failure and reputation) were commonly identified as the most difficult or impossible risks to insure, suggests insurers are failing to address some of the major concerns for risk managers at financial institutions. One respondent summed it up as: "Insurers and brokers are no longer thought leaders in risk management. They are merely a commodity in any risk management solution. For 70% of a firm's exposures, most insurers have no solution."

Conclusion

The economic crisis of 2008 plunged the financial sector into chaos. The aftermath has resulted in a more complex risk landscape where compliance is key.

Indeed, regulatory reform is a major concern for risk managers and is also a main driver behind improvements in risk management within FIs.

Although positive, this trend also raises questions as to whether top executives really appreciate the benefits of risk management or whether they are merely responding to pressure from regulators to increase risk reporting. By doing so, FIs will certainly have ticked a box, but this says little about whether risk management is really valued.

The question risk managers should perhaps be asking themselves is whether senior management would invest in their function if such regulatory pressures did not exist.

For some FIs, it seems that the main driver for change is the threat of enforcement, rather than a willingness to invest in risk management to promote best practice. Irrespective of what the correct attitude might be, it is clear that much remains to be done to raise the standards of practices in the financial sector. SR

40% say *insurable* exposure accounts for between 20%-30% of overall **risk profile**

49% identified capital requirement as ***number one concern***

Claims service considered the second *most* ***important*** factor of a **policy**

53% said the **financial crisis**, ***had made business*** more **risk-averse,** but...

...28% identified ***no change***

THE RISK MANAGERS' VIEW

Risks uncovered

Five industry insiders explain which are the main risks faced by their sector

Michel Maila,
President and chief executive at Global Risk Institute, former vice-president at IFC

It is important to distinguish between risks and emerging risks.

Regulatory change is a familiar risk, although the pace of change has increased since the financial crisis of 2008. It is part of the business of regulated banks or insurance companies to deal with the regulators. However, cyber security is an important emerging risk with which financial institutions (FIs) are not yet familiar because hackers are innovating. System failure is a familiar risk and all FIs have been investing heavily in information technology and other systems, so for them.

Two further emerging risks present significant challenges for FIs. The first is the end of low-level interest rates. This raises questions such as if and when we will return to normal and how orderly will that process will be.

The answers are unknown because jurisdictions such as the euro area, the US and Japan have never experienced six years of near-zero interests rates.

The second emerging risk is market liquidity, which is drying up in a number of markets, particularly regarding corporate bonds, but it is relevant across several different bond sectors. It is a significant concern because the notion of a resilient financial system depends critically on market liquidity. How can there be a safer more resilient system if transactions become more difficult?

Gustavo Benedetti,
Chief executive Darep Ltd at Groupo Santander

In my opinion regulatory change is not a risk: it is a challenge that needs to be managed to be compliant; if it becomes a risk it is because companies are doing something wrong.

Cyber is the most concerning risk, although it is not a new risk. However, it has become such a sophisticated crime that it is dangerous and challenging for industries such as ours because, to be competitive, we depend heavily on information and technology.

Much like anything humanity does, we constantly invent faster, better things. However, eventually, it becomes clear that the new faster and better thing comes with a new set of challenges, which by virtue of not having existed before, could not have been predicted properly. This process happens over and over again. Someone will always find a solution but, in the meantime, insurance will usually try to cover the gap.

Every institution needs a general framework of action for risk management, but risk managers need to be aware of the local, national and regional laws.

There should be common principles and a common risk appetite across the organisation, but risk management teams need to be adapted to the local risk landscape, where there are often differences in regulations.

Emmanuel Fabin,
Insurance manager at TSB Bank

How can insurers better support FIs? The market and organisations need to improve.

Professional indemnity has always been a high-profile element of insurance, even before the credit crunch, but it has become a bigger issue since the crisis. Now, the robustness of regulators is increasing, particularly with retrospective analysis of conduct risks (the risks associated with how a firm and its staff conduct themselves). Regulators are looking at issues that do not necessarily reflect the current risk culture and the risk management of FIs, but they are focusing on issues of the past 10 to 15 years.

For large FIs, there is such a large value attached to managing conduct risks, but is there a form of risk mitigation that is useful for large multinationals?

The survey shows that for 40% of FIs, their insurable risks make up between 20% and 30% of their overall exposures. This could be improved, but it depends on the levels of engagement between a firm's operational risk function and its insurable risk function and then how it articulates its communication to the insurers.

However, there seems to be a disconnect between insurable and non-insurable risk functions. This is not because risks are non-insurable, but because the language of insurance is often not translated to a language that operational risk personnel understand. The figure of 20% to 30% shows that some FIs are doing this better than others and some are not taking the right approach.

Ian Davies,
Head of risk Europe
at Schroders

Regulatory change is top of the agenda for management and being able to respond to this correctly is critical for financial services. Hopefully firms are operating the way regulators envisaged it. For example, the protection of client assets, designing and selling appropriate products to investors and ensuring that products are managed within their risk profiles are sound business practices that firms with integrity should be doing. However, the requirement to document compliance with regulations in areas such as the Alternative Investment Fund Managers Directive is more onerous. This directive meant firms had to make expensive system changes to be compliant.

Cyber risk is one of the greatest current issues, although other risks are also recognised. As the survey shows, cyber risk is particularly concerning owing to the evolving nature of the threat. The traditional view of hacking (the lone geek in a bedroom), has evolved. Now, more resources are being brought to bear from criminal organisations and nation states. Motivations for cyber attacks have also changed from those who cracked systems to prove that they could do it, to politically driven motives.

Challenges likely to emerge in the next 10 to 15 years relate to the asset management sector, which is under a lot of pressure on margins, from multiple sources: regulatory costs, political pressures and low-cost tracker products. Financial services will further consolidate to achieve economy of scale, bear the cost of regulations and systems and build resilient balance sheets.

Guenter Droese,
Former managing director
of Deutsche Bank AG

When assessing the threats to financial institutions, the first question I would raise is regarding the organisation's strategy and business plan. What type of banking activities are relevant to that particular institution?

The lessons learnt from the past 15 years should be to consider not only the risks that need to be measured for Basel II or III, such as credit market and operational risk. Financial institutions should investigate and discover what the general threats to banking activities are.

Most of the banks that contributed to the financial crisis still behave in the same or similar manner. Many of these transactions, which were crucial for the banks' competitiveness, are still being made now in the grey market without any control.

There are plenty of discussions regarding the earnings of investment bankers, who still receive huge bonuses even when something has gone wrong. The big banks are circumventing various kinds of rules on this. The more this becomes public and transparent, which is not happening at the moment, the more it becomes a significant reputational risk for the banks. Bank managers should be taking a long-term view about securing good relations with the entire customer base, but I do not believe the majority of banks understand this.

How risk managers rank the value of the following insurance (1-10):

- Cyber: 5.47
- Operational risk: 5.21
- International programmes and out-of-territory compliance: 5.47

Factors of most importance to risk managers (1-10):

- Insurance price: 6.85
- Insurer's expertise and knowledge: 7
- Insurer's service level: 7.38
- Range of products: 5.55
- Relationship with underwriters: 6.55
- Access to a relationship manager: 6.08
- Insurer's financial rating: 6.9
- Insurer's overall reputation: 6.10

INTERVIEW

Learning the lessons

The past 15 years have seen a plethora of banking scandals and many more continue to emerge, which begs the question as to why history keeps on repeating itself. Here, Nick Leeson, who brought down Barings Bank in 1995, talks of his experience and explains why financial institutions seem to carry on with the same erroneous ways

From the Lehman Brothers collapse in 2000, the $2.3bn-worth (€1.8bn) of losses suffered by UBS as a result of risky bets made by rogue trader Kweku Adoboli in 2012 to the $920m fine given to JPMorgan Chase in 2013 for losses connected to the 'London Whale' trades, the past 15 years have seen some of the biggest banking scandals to date.

Unfortunately, these will not be the last banking crimes, as some of the world's top banks brace themselves for millions of dollars worth of litigation losses related to alleged cases of foreign exchange rate fixing.

Despite tougher legislation laid down by regulators, cases of wrongdoing among financial institutions (FIs) continue to surface. It therefore begs the question as to why lessons from the past have not been learnt.

Nick Leeson, who brought down the 233-year-old Barings Bank in 1995 after accumulating $1.3bn of liabilities (more than the entire capital reserves of the bank), answers the question simply: "It's down to poor systems, poor controls and poor quality of people."

Drawing on his experience as a rogue trader at Barings Bank in Singapore, Leeson gives his candid views as to why FIs continue to commit these crimes.

"I'm not suggesting I have all of the answers, but I can speak honestly about what went wrong during my time at Barings Bank," he says. "Much of it was my fault, but the structure [of the bank] had many organisational flaws and the quality of people in certain positions was not what it should have been. A lot of these errors apply to more recent scandals."

Leeson revealed everything in a Q&A with *StrategicRISK* before his keynote speech at the *StrategicRISK*-Zurich financial institutions forum.

The past decade alone has witnessed some of the biggest financial scandals and collapses to date. Clearly, lessons have not been learnt, have they?

Lessons have been learnt, but they are forgotten quickly. That's just human nature. Each scandal serves as a reminder that we should have learnt better. Making a mistake once is acceptable, but making the same mistake again is stupid and unjustifiable.

Cases such as Jérôme Kerviel at Société Générale, Bruno Iksil at JPMorgan Chase or more recently the manipulation of the foreign exchange rate show that the potential for another global upheaval is apparent.

All financial scandals are same; they just differ in terms of degree of complexity and level of deception. Why these are allowed to happen always boils down to three main errors: poor systems, poor controls and poor quality of people.

Should poor risk management be added to your list of errors? Lax risk management is often cited as a reason for why things have gone wrong.

The problem is that risk management is an evolving discipline, but it is not evolving quickly enough. The function is a work in progress, but it's nowhere near where it should be. The issue is that financial markets are developing at a faster speed than risk management.

Risk management has to evolve at the same speed, if not faster, than financial markets. Otherwise, there will always be a disproportionate amount of risk. It is a classic tortoise and hare example, where the hare (financial markets) is racing ahead of the tortoise (risk management).

Do you think that risk managers are receiving adequate support from the board to really fulfil their roles and help prevent problems?

Not receiving the right support is a key element, but the question should be why they are not receiving it. Typically, it is because it costs businesses money to invest in risk management and the returns are not immediate.

Unfortunately, when executives and board members decide where to invest their money – in risk management or in the trading desk – they will opt for what will make the most money and therefore choose the trading desk.

What about the regulators? The 2008 financial crisis exposed how weak the regulatory framework was. It is not helpful if risk managers and regulators are one step behind...

The problem is that few talented people are going into roles at regulatory bodies. Typically, the highest calibre of people go into the trading environment, the next calibre choose risk management and then someway down the path some people become regulators.

When I worked in Singapore, there was a shortage of good people in these roles. It was a process of 'natural selection'. When banks needed to hire, they looked to other firms. When nobody from other organisations was suitable, they searched for people from the regulators and auditors.

Alternatively, if an auditor was recruited, did a particularly good job and the bosses deemed them to have potential, they would often get recruited onto the trading desk. This level of poaching weakens the regulators and, all of a sudden, there are few high-calibre staff regulating, risk managing or auditing.

What can banking bosses do to prevent the next scandal? Often, when a rogue trader has been exposed or a case of wrongdoing surfaces, executives are said to have to 'turned a blind eye'. Is this fair?

Executives and all employees should be challenging decisions and actions. Executives should challenge from the top down and employees should challenge from the bottom up. However, for this to happen, the right culture needs to be in place so that all members of staff feel empowered and sufficiently comfortable to communicate their concerns.

When I worked at Barings Bank, the point of referral was not a nice person. This worked in my favour because if anyone had had an inkling as to what I was doing, the point of referral would be the last person they would go to.

Would you have done things differently had you been challenged?

Absolutely. During my time in Singapore, I survived day by day and as no one was questioning what I was doing, I became more comfortable – not comfortable with what I was doing, but comfortable with the idea that I had some more time to correct it. After a while, I started to think in terms of three- or four-day periods. I was supplying figures to the accountant that did not make any sense, but they just accepted it, and so I felt I had weeks to sort out the mess. Then, when auditors came in and they did not expose anything, I began to think I had months to fix the problem. If errant behaviour is not punished, another employee might witness it and copy the behaviour.

So, what does good corporate governance look like?

Good governance is having a culture where departments look over the organisation, ask intelligent and challenging questions, rather than having departments that look at sheets of numbers and tick a few boxes.

What does a good risk manager like? They will be someone who challenges the organisation and members of staff everyday. However, what risk managers tell me is that they are so weighed down with paper work, box-ticking and filling in reports merely to comply with the latest legislation, that they do not have the opportunity to challenge anyone or anything the way they should.

It is important that risk managers are in positions of authority and have a voice within the organisation. I have heard of so many cases where risk mangers have been ignored, where they have provided reports to boards and have been told that they are wrong. If risk managers report to non-executive directors who are more responsible and culpable for what goes wrong, then maybe more will be done to prevent cases of fraud and scandal. **SR**

CYBER RISKS


Shutterstock

The most hazardous space

As the threat from fraudsters, hacktivists and hostile governments increase, financial institutions need to upgrade their cyber defences constantly. But what – if any – protection can the insurance sector offer?

In less than a decade, cyber risk has grown from an emerging and little-understood risk to a pressing concern on a global scale. The risk is attracting board-level attention across industries and, in particular, at financial institutions (FIs).

This is reflected in the results of our survey (see pp4-5) in partnership with Zurich, in which risk managers at FIs identified cyber as the second most concerning risk for the industry, after regulatory change.

Cyber risk was perceived as one of the main five threats to FIs by 65% of respondents and one-third had cyber as either the first or second biggest concern for FIs.

A significant factor in cyber risk is that it encompasses various risks. An attack can result in, for example, reputational damage, business interruption, regulatory penalties and loss of critical information. Furthermore, cyber attacks are increasing in frequency and sophistication.

"There is a proliferation of people who have the capability to carry out a cyber attack, which is a big part of the problem," says James Hatch, director of cyber services for BAE Systems.

Individuals actively involved in cyber attacks on FIs are, however, motivated by various different reasons, which dictate the level, type and scope of the risk they pose.

Retail banks, for example, have long been targets for criminals motivated by financial gain, and cyber space provides a platform from which they can infiltrate banks and extort money. Similarly, insider fraud is an ever-present concern across the financial sector, as are state-sponsored attacks and crimes motivated by political and ethical reasons.

Insider and outsider threats

Massimo Cotrozzi, assistant director of EY's fraud investigation and dispute services team, says about 90% of fraud is committed using cyber methods. "In an increasingly digital world, where processes are carried out through computers, risks arise around security and hacking," he explains.

Although FIs have mechanisms to detect fraud, he says many do not have a system that correlates internal and external threats that could be working in tandem.

"Organisations may not know if someone is doing something on the outside that corresponds to malicious activities on the internal network or totally legitimate activities, inside or outside, that, when linked together, make for a malicious outcome," Cotrozzi says.

An extension to this aspect of cyber risk is human error. Failing to follow security protocols and ordinary human fallibility can damage internal systems and put valuable company data at risk, according to Hatch.

"Humans are a key element to cyber risk; not only the known criminals and insider crime, but also people going beyond what they need to do and being careless or misguided," says Hatch.

The risks attached to insider and outsider cyber crime and human errors are primarily related to the potential for financial losses. In April 2013, for example, a well-known UK bank reported losses of €1.67m from customer accounts after a gang member disguised as an IT engineer covertly installed hidden cameras in its computers.

Individuals and groups motivated to attack FIs for ethical or political reasons pose a different threat. These individuals, known as hacktivists, have a more antagonistic approach and are more likely to draw attention to their activity in the hope that it will inflict significant damage to an organisation's reputation.

Hacktivists may target FIs with the aim of weakening the critical infrastructure of national and global economies. It is an industry-wide threat to which organisations, particularly in major economies, need to be alert.

"Banks and insurers have been at the front of this. Now other parts of the finance sector must worry about their cyber security to a greater degree," says Hatch.

In a similar vein, state-sponsored cyber attacks are a growing concern among critical infrastructure firms. Indeed, geopolitical tensions between the West, Russia and China, among others, are quietly increasing the risk level for FIs.

Recent attacks on several major US banks, including JPMorgan Chase, aroused suspicions in the media that the culprits may have been based in Eastern Europe. Although no official statements were made to support such assertions, the FBI is now investigating these incidents.

Earlier this year, the US and China became embroiled in a dispute regarding cyber espionage, with each side accusing the other of spying through cyber space. It puts FIs in an increasingly precarious position and enhances their status as potential targets for politically motivated and state-sponsored hackers.

"Many of our customers are becoming more interested in the political risk that is related to the cyber space," says Hatch. "An attack may have nothing to do with the organisation, but it may get caught in the middle of political cyber warfare.

"Larger organisations are now setting up intelligence capabilities that are closer to what traditionally has been done by national security than commercial business, although different techniques and legal frameworks apply for them."

The increasingly broad scope of cyber exposures for FIs arguably presents insurers with an opportunity to support clients. However, the market appears to be stuttering in its attempts to produce viable risk transfer solutions.

In our survey, 53% of respondents said cyber risk was either difficult or impossible to insure and 51% said the same of system failure.

Insurers may be taking the wrong approach, according to Hatch, who says many are focusing too heavily on business interruption through cyber means. Nonetheless, he remains confident the market will produce valuable risk transfer products in the near future.

"The insurance sector will provide products where there is a market that needs them. As the risks evolve, I'm sure the insurance market will evolve with it," he says.

In the meantime, it is important that FIs optimise their risk management capabilities and minimise cyber risk exposures.

"A key part of cyber risk is clarity of responsibility," says Hatch, but, he adds, delegating the responsibility of cyber risk management among the workforce is possible only when the organisation's exposures are fully understood. That means considering various seemingly unrelated factors such as a firm's corporate history, geographic location, brand position and internal system structure.

"Once you understand the shape and size of a risk, you have the basis on which to make decisions," Hatch says.

A common mistake for many FIs is failing to account for unknown cyber threats, according to Cotrozzi. He says risk assessments often fail to include unknown threats, such as new types of cyber attacks or techniques used by fraudsters that are so far undetected.

"This is why firms must perform a risk analysis and a threat analysis," says Cotrozzi. However, detecting and preventing cyber threats is only part of managing the risk.

Prevention is key

"The increasing number of cyber attacks means firms must be more prepared to deal with their consequences, as well as trying to prevent them," says Hatch.

Cotrozzi agrees, giving a frank assessment of the situation for FIs: "FIs should assume their systems will be compromised and breached. They should assume someone will try to defraud them and that they need to monitor the indicators that will bring it to their attention.

"Every threat cannot be prevented and 100% of breaches cannot be fully remediated. Sometimes, it's too complicated."

FIs depend on the efficiency and security of digital communication and cyber space, where weaknesses can damage a firm's reputation significantly and leave it vulnerable to financial losses.

"For FIs, their safety and trust is very important and reputation damage is one of the main consequences of cyber losses or incidents," says Hatch. For this reason, FIs are prime targets for political hackers.

At the same time, cyber space has become a testing ground in which criminals can not only innovate but also refine their operations.

As a result, FIs must be prepared to invest consistently in improving cyber defences while engaging in a seemingly never-ending battle with hackers, hacktivists and fraudsters. **SR**

THOUGHT LEADERSHIP

TIM STAPLETON
Global underwriting manager at Zurich General Insurance

NEED-TO-KNOW BASIS

It is not surprising that cyber risk was identified as one of the top five threats for financial institutions. These businesses are under constant attack and it is inevitable that perpetrators – whether internal members of staff or external hackers – will succeed to harm the company and/or steal data.

It would therefore be more effective for businesses to consider how best to manage a cyber-related breach or attack once they have occurred in addition to applying preventive measures.

One of the most effective methods against insider fraud in particular is to enforce what is known as 'least privilege' or need-to-know accessibility. These policies stipulate that each employee is provided with the least set of privileges or access to restricted or sensitive information necessary to complete the job. Some companies have fallen short by providing too many employees and third parties/independent contractors with full access to sensitive data, which is not needed to do their jobs.

For other cyber attacks, companies should segregate their data so that sensitive information is not kept in one place. Thus, if an attacker manages to break into certain systems, they are limited in what they can access.

Further, encryption is one of the most effective mitigation strategies available. A lot of attacks are smash-and-grab incidents, where perpetrators get in, take as much information as they can and then get out. Hackers are generally looking for a target of opportunity and plain text data is a higher target of opportunity than protected and encrypted data.

Malware protection and prevention is also vital. Many data breaches in the retail sector are caused by malware that sits on the companies' systems and networks for months without detection. Malware detection software and patch management (procedures and technologies responsible for keeping computers current with updates) – are key in preventing such attacks.

Last, third-party vendors have accounted for a high percentage of breaches. In many cases, companies are not adequately vetting the information security and privacy risk management controls that third parties have in place and to whom they entrust sensitive information. It is important to have a stringent set of criteria in place to use as a basis for evaluating new and existing vendors and business partners. In addition, it is best practice to specifically address indemnity and insurance protections in contracts in case of fraud or data breach issues.

BASEL III AND BEYOND

Aiming for stability

European regulators have been busy since the financial crisis reforming financial markets to ensure they are better prepared to withstand future turmoil, improve governance and enhance their disclosure procedures

Regulators came under attack when the financial crisis of 2008 exposed grave weaknesses in the global regulatory framework and the risk management practices in banks and financial institutions (FIs). This prompted authorities to review existing requirements and propose new measures, the most prominent of which is perhaps Basel III, a regulatory framework that aims to increase the stability of financial markets.

Cutting through the complexity of Basel III formed the basis of two sessions at the financial risk forum. Steven Hall, partner in financial risk management at KPMG UK, gave an overview of Basel III and of the likely regulatory changes in 2015, and Syril Pathmanathan and Dimitris Bartzilas, from the risk-weighted assets (RWA) optimisation and operational risk departments at Crédit Suisse, looked at the effect of Basel II and III on FIs. This article summarises the key points.

Although it was agreed in 2010 by the Basel Committee on Banking Supervision, Basel III was introduced from January 2013. Its principal aims are to:

- improve the banking sector's ability to absorb shocks arising from financial and economic stress;
- improve risk management and governance;
- strengthen banks' transparency and disclosures; and
- strengthen global capital and liquidity rules.

Banks are expected to phase into Basel III in the next four years and to have fully implemented it by 2019.

Under this regime, banks will have to adhere to several new or enhanced rules, which include a clearer definition of capital and the introduction of a global liquidity standard.

Capital requirements rules

The crisis showed inconsistencies in the

definition of "capital" across Europe as well as a lack of disclosure among banks that would have enabled the market to compare the quality of capital. As a result, the Basel Committee clarified the definition of "capital" with a greater focus on "common equity" – the highest quality component of a bank's capital. The new definition requires:

- common equity tier 1 (CET1) to be at least 4.5% of RWA, that is the bank's assets weighted according to risk;
- tier 1 capital to be at least 6% of RWA at all times;
- total capital (tier 1 capital plus tier 2 capital) to be at least 8% of RWA at all times; and
- an overall CET1 ratio of 7% by 2019 to avoid restrictions on the payout of management bonuses and dividends.

How the banks responded

In September 2014, the Basel Committee published the results of the latest Basel III monitoring exercise, which took place in December 2013. This showed that European banks are on track to meet the capital requirements.

A total of 227 EU banks participated in the exercise, comprising 102 global banks with a tier 1 capital exceeding €3bn, referred to as "group 1 banks", and the other 125 banks are referred "group 2 banks" (that is, all other banks).

According to the monitoring results, group 1 banks would have a shortfall of €100m for the CET1 minimum capital requirement of 4.5%, which rises to €15.1bn for a CET1 target level of 7%.

The capital shortfall for group 2 banks is estimated at €2bn for the CET1 minimum of 4.5% and €9.4bn for a CET1 target level of 7%.

Speaking at the *StrategicRISK*-Zurich forum, Hall said: "It is clear that for some banks there is a significant shortfall to those capital requirements, but those shortfalls have come down considerably since last year.

"Indeed, if you looked at these shortfalls in comparison to the annual profits of the banking sector or the banks represented here, this would be a small proportion of those profits.

"So, these firms are on their way to meeting the minimum requirements."

He added: "There is also quite a difference between different regions around the world. So, European banks tend to have lower CET1 ratios than Far-Eastern banks, for example, primarily because they were far more equity-funded already and therefore they have had less far to go in terms of meeting the requirements."

Beyond Basel III

Although it would seem that banks are making good progress in meeting the Basel III requirements, there have been several modifications to certain elements of Basel III and, with further consultation taking place on other aspects of the regulation of FIs, further reforms can be expected.

Hall highlighted some of the main changes that have taken place and some future modifications.

Large exposures

In April 2014, the Basel Committee published the *Supervisory framework for measuring and controlling large exposures*.

The framework is expected to take effect from 1 January 2019 and aims to protect banks from significant losses caused by the default of an individual counterparty or a group of connected counterparties.

"Large exposures would have a particular impact for the larger banks," Hall explained. "The framework could restrict further the interbank lending, which is going to create further issues in respect to how banks deal with major broker dealers."

Central counterparties

The Basel Committee, the Committee on Payments and Settlement Systems and the International Organization of Securities Commissions set out to improve the interim capital requirements for bank exposures to central counterparties (CCPs). CCPs are organisations that exist in various countries that help facilitate trading done in derivatives and equities markets.

In July 2012, the Basel Committee published an interim standard for calculating regulatory capital for banks' exposures to CCPs. This was introduced by additions and amendments to *International convergence of capital measurement and capital standards* (known as Basel II).

In April 2014, the final standard, *Capital requirements for bank exposures to central counterparties*, was published. It will take effect on 1 January 2017, and the interim requirements will apply until then.

Securitisation

In December 2013, the committee issued a consultation on revisions to the securitisation framework.

Securitisation is the process through which an issuer creates a financial instrument by combining other financial assets and then marketing different tiers of the repackaged instruments to investors.

Hall said: "Securitisation has had a negative reputation in the past few years. It is considered by some to have caused many problems in the financial crisis, but I believe regulators and policymakers have realised they need to encourage securitisation to ensure real economy financing and we have seen a new capital regime for securitisation", which should be finalised in due course.

TLAC (total loss absorbing capital)

TLAC is the new capital requirement proposal for large banks. Under this requirement, banks will potentially be required to hold 16% and 20% of their RWA. "This will again put further pressures on large banks returns on equity numbers," Hall said.

RWA review

Regulators are conducting a review of the RWA regime.

The objective of this review is to identify any differences in RWA outcomes, to understand the sources of such differences and, if required, to formulate the necessary policy solutions to enhance convergence between banks and to improve disclosure.

What else is in the pipeline: Basel III

Hall said there were strong signals of a new conceptual framework for capital standards, which he referred to as 'Basel IV'.

He said Basel IV would have three major implications:

- banks are likely to face significantly higher capital requirements;
- banks will likely need to improve their capital management; and
- a less risk-sensitive approach to both capital ratios and internal modelling is likely to force banks to re-evaluate the balance between lower and higher risk businesses.

More changes to come?

Looking to the year ahead, it seems the regulatory landscape is likely to become more complex. Hall said: "Basel III has had a big impact well ahead of the final implementation date with significant capital raising.

"This is not the end of the story. With a wide range of parallel and future proposals in the prudential regulatory space taking place, the attention must turn to the effect on the wider economy and what the agenda for financial services should be to support those wider jobs and growth agenda." SR

REGULATION

Keeping up with the law

Regulatory change is a major concern for financial institutions, from an increase in EU rules to the US becoming an over-regulator

The 2008 financial crisis exposed devastating flaws in the regulation of financial institutions (FIs) and shook the global economy in the process.

Corporates and states were badly affected and the financial sector bore most of the blame for the downturn. In response, regulators have endeavoured to reshape the financial system, reinvigorate economic growth and avoid a repeat of the crisis.

Notable reforms to the regulatory landscape include Basel III, which was introduced by the Basel Committee on Banking Supervision to increase the resilience of global banks in periods of stress by improving governance, risk management and transparency. Another prominent reform is the Solvency II Directive, which aims to guarantee insurers' ability to pay claims.

Six years after the crisis and regulatory reform of the financial sector is showing no sign of easing. In October 2014, the European Commission adopted a delegated act and a draft proposal for a Council-implementing act to calculate the contributions of banks to national resolution funds and to the newly created Single Resolution Fund (SRF) respectively.

The SRF is part of the Single Supervisory Mechanism (SSM), under which the European Central Bank becomes responsible for supervising the largest banks in the euro area from November 2014, among other things. Its purpose is to ensure an orderly resolution of failing banks with minimal costs for taxpayers and to the economy. As such, the SRF ensures the availability of medium-term funding to banks in financial difficulty covered by the SSM to enable them to continue operating while being restructured.

The SRF is due to start on 1 January 2016 and banks subject to it will have to contribute in proportion to their sizes and risk profiles.

Non-compliance

The penalty for breaching regulations can be costly. For example, the Financial Conduct Authority, the UK financial regulator, handed more than €385m worth of fines between January and October 2014.

The largest of those was a €132m fine paid jointly by Lloyds Bank and Bank of Scotland (Bos) for serious misconduct relating to the Special Liquidity Scheme (SLS), the Repo Rate benchmark and the London Interbank Offered Rate.

The SLS was introduced in 2008 to improve the liquidity of banks by allowing them to swap some of their assets that are currently illiquid for UK Treasury Bills for up to three years. Lloyds and BoS were found to have manipulated the repo rate, which determined the short-term fees payable to the government for their participation in the SLS.

Indeed, regulatory change is a major concern for FIs. This was reflected in our survey of senior risk managers, in which regulatory change was identified as the top risk for the financial industry: see pp4-5.

With regulation high on the list of priorities for risk managers, delegates at the Financial Institutions Risk Forum discussed the evolution, purpose and necessity of regulation in the industry in a dedicated risk clinic.

A world without regulation

The evolving regulatory requirements for FIs risk clinic was led by Richard Tall, partner and head of financial regulation at law firm DWF.

Tall opened the discussion by asking delegates to consider the necessity of regulatory bodies and what business would be like in a world without regulations.

"It's a debate between free markets and some kind of intervention. Generally, a balance is required and I don't think we have found that yet," said Arooran Sivasubramaniam, Zurich Global Lines Pricing financial lines lead.

The position of financial regulators is central to modern society, according to Tim Atkin, Zurich Global Corporate head of customer, distribution and marketing EMEA.

He said: "If there is no penalty for failure, then you remove one of the fundamental checks and balances of the capitalist environment.

"That means underperformers are likely to continue to underperform and deliver a substandard service because there is no penalty for failure."

A key issue for multinational FIs is the jurisdictional differences between the countries in which they operate. Of particular concern is the over-aggressive US approach to financial regulation, which is "as much about protecting home markets and creating barriers to trade as


Shutterstock

it is about protecting the end user," according to one delegate.

"Does the US want to become the world leader in regulation and expect other regulators to follow?" asked one delegate who wanted to remain anonymous, adding: "I feel we are not pushing the US enough to prevent it from becoming an over-regulator."

Moreover, the Federal Reserve has introduced a rule that stipulates US operations of non-US banks with more than $50bn (€40bn) in global consolidated assets must hold risk-based capital, liquidity and leverage similar to their US peers, with effect from 1 July 2016. It means some banks may need to set up separately capitalised intermediate holding companies for their US subsidiaries. In July, the US rejected EU proposals to include co-operation of financial regulators in the Transatlantic Trade and Investment Partnership discussions.

Another delegate said: "I don't think the end consumer necessarily sees many benefits for many of the regulations that are supposedly done in their name [by US authorities]."

Tougher legislation

Political expediency of regulations by policy makers was also discussed.

Delegates agreed that governments benefit by backing stringent regulations on FIs as this forces them to take some responsibility for economic stability.

Tall reminded delegates of historic crises that are comparable to the 2008 financial crisis, including the Dutch tulip scandal of 1637 and the South Sea bubble in 1720. The latter paved the way for the establishment of a financial services regulation system, according to Tall, after British parliamentarians lost conssiderable sums of money.

As society has grown in complexity, so too have the laws and regulations designed to maintain and protect it. Considering the number of recent scandals, such as the manipulation of the foreign exchange rate, perhaps tougher legislation is necessary to protect the world's economy. As Atkin alluded to, regulators are central in a risk landscape that is so complex. **SR**

StrategicRISK

Editor
Mike Jones

Deputy editor
Kin Ly

Managing and legal editor
Hélène Préchac

Asia editor
Sean Mooney

Reporter
Asa Gibson

Business development manager
Eric Anderson

Commercial director, Asia-Pacific
Adam Jordan

Senior production controller
Alec Linley

Senior data analyst
Fayez Shriwardhankar

Publisher
Tom Byford

Executive publisher, Asia-Pacific
William Sanders

Managing director
Tim Whitehouse

Published by
Newsquest Specialist Media Ltd
30 Cannon Street, London EC4M 6YJ
tel: +44 (0)20 7618 3456
fax: +44 (0)20 7618 3420 (editorial)
+44 (0)20 7618 3400 (advertising)
email: strategic.risk@nqsm.com

For all subscription enquiries please contact:
Newsquest Specialist Media, PO Box 6009,
Thatcham, Berkshire, RG19 4TT, UK
tel: +44 (0)1635 588868
email: customerservice@strategicrisk.eu
Annual subscription (incl P&P)
£249 €399 $499
Two-year subscription
£449 €649 $849
Three-year subscription
£427 €663 $821

Printed by Warners Midlands Plc