Question time: Werner Bijkerk, head of research of IOSCO on cyber crime in the securities market

Mar 06 2014 Patricia Lee, Compliance Complete

Cyber security in the financial system has emerged as a significant risk in recent years. The risk of cyber crime in the securities market, in particular, has begun to attract the attention of regulators and market participants alike. Regulators and standard-setting bodies such as the International Organisation of Securities Commissions (IOSCO) are now putting more emphasis on this growing threat which, if left unchecked, could cause disruptions not only to the financial system but also to the entire economy.

Werner Bijkerk, IOSCO's head of research, talks to Compliance Complete about IOSCO's latest work in tackling cyber risk in the securities market, and global regulators' efforts in addressing this risk. In the first part of this interview, Bijkerk discussed crowd funding.

Cyber security risk has been singled out as a top systemic risk by many surveys but we have heard little about cyber risk in the securities market. How serious is cyber crime in the securities market?

IOSCO's research work identifies emerging and potential systemic risks. We carry out a lot of different exercises, and we send surveys to market participants to help us detect emerging and potential systemic risks. Two years ago when we received the results to our surveys, only one respondent highlighted the risk of cyber crime. At the same time, however, one of our regulatory experts also highlighted cyber crime as a concern and pointed to stock exchanges being hit by cyber attacks. Our research department realised that cyber crime was a topic that we did not have a full understanding, and so we decided that this was an area where we should focus our attention.

This led us to work with the World Federation of Exchanges, which had also recognised the risk of cyber crime. Although it was not the task of the World Federation of Exchanges (WFE) to address cyber crime in the securities market, it wanted to find out more. Together the IOSCO research department and the WFE secretariat developed a survey to be sent to the world's exchanges and we wrote a staff working paper which is now seen as leading in discussions on cyber security risk in financial markets globally.

In December 2013, the WFE set up the Global Cyber Security Committee. In the same year, the Committee on Payment and Settlement Systems (CPSS) also set up a committee that looks into cyber crime in financial market infrastructures, including exchanges, as well as clearing, payment and settlement systems.

At IOSCO, we have a specific function and that is to identify systemic risks. We asked the World Federation of Exchanges if it could send our surveys to its exchange members. After the publication of our staff working papers in July 2013 on "Cyber Crime, Securities Market and Systemic Risk", we started to get a lot of responses from other global regulators. Last year we presented our survey results to the European Central Bank, and next month we will be presenting a report on cyber crime in the securities market to the Systemic Risk Board.

People used to think that cyber threats were an IT issue, and therefore only of interest to IT experts. It is In fact a threat that can bring down an entire exchange or a clearing house. It is more than just an IT concern and that was a big finding in our report – that it is a systemic risk. We have interviewed experts from around the globe and they came to the same conclusion: that it is not just something for the IT nerds [to handle], but that it is a real risk waiting to happen and should be a top agenda of chief risk officers.

If you think of the banking regulations, they largely concentrate on financial risk, the balance sheets of banks and their risk models. But in cyber crime, there are no risk models. Cyber crime is entirely an operational risk and has the potential to bring down a bank. When accounts are hacked into, this is only a relatively small aspect of cyber crime.

What did the IOSCO research findings say about the motives behind cyber crime?

Criminals are looking beyond financial gains. They may have political motivations or they may be cyber spies who are looking to steal economic secrets from firms and nations. Terrorists and nation-states both use cyber threats to disrupt and to destroy. Our research findings also showed that insiders in firms who sought to steal or sabotage often became involved in cyber crime. Cyber attacks are so easy to carry out that even students can perform this kind of activity.

How prepared is the world for cyber attacks?

In the securities market, exchanges now are run totally on IT systems. They are technology hubs with the most advanced technology that run all kinds of trading platforms, including high-frequency trading. In the last couple of years many exchanges have made their systems and risk controls much more sophisticated. They have invested a lot of efforts and resources to protect their systems and have engaged very experienced people from national defence and cyber defence to help them with their systems. Banks and financial institutions have done the same.

Are we ready? We certainly are not ready. The methods employed by cyber criminals are constantly developing. They have the power to destroy and that makes cyber crime very dangerous. Regulators and industry players have recognised this risk as the least controllable and one of the most aggressive. It is also very hard to track where the attacks are coming from; they can come from anywhere in the world. Even if we are able to track the attacks it is hard to know how to stop these people or groups from doing harm. This is a global playing field without global rules nor indeed global courts from which to carry out prosecutions.

How effective are regulations in preventing cybercrime?

Let's try to put some figures here. In 2012, 53 percent of the world's exchanges reported that they had experienced cyber attacks. Yet our studies revealed that most exchanges (about 95 percent of them) do have protection and preventative measures. They have disaster recovery measures in place, they train their staff on cyber security risk and they also have documentations to address cyber threats. But sharing of information among regulators and authorities is also very important. The fact that the way cyber attacks changes and innovates from day to day means that we need to exchange information to know what is going in order to protect our securities markets.

About 60 percent of the exchanges reported that in their jurisdictions they had sanctions regimes with some kind of laws and regulations in place. Of the 60 percent, however, only half of the exchange said that sanctions regimes were effective in deterring cyber crime because it was cross-jurisdictional in nature. That makes attributing the source of the cyber attacks difficult. The other aspect of regulation is whether regulators actively oversee institutions and ensure that they have protective measures in place.

At IOSCO we started a work stream on electronic trading in the beginning of this year. The work stream seeks to understand how market operators, including exchanges, dark pool operators and financial intermediaries such as broker-dealers, operate. The work stream will get them to identify critical systems, map the requirements relating to the systems, and then identify security measures and standards to prevent unauthorised access. This mandate is carried out by the IOSCO Policy Committee of Secondary Markets, which will develop global policies against potential cyber risk. These principles will help to detect, prevent and offset the risk of cyber crime, and they will undergo a public consultation in December 2014.

In addition, IOSCO, together with the CPSS, will develop principles on financial market infrastructures. IOSCO and the CPSS have recognised the importance of setting out global principles for cross-jurisdictional risk, which is why they are looking at launching the work stream. The work stream will target all financial market infrastructures, including market operators, clearing houses, payment and settlement systems such as SWIFT.

What is the level of awareness on cybercrime at the state level, by regulators and market players?

Cyber crime is not a risk that can just be left to the IT experts; it is a risk for the firm, the financial system and society as a whole. These days, financial institutions are highly dependent on IT and it is important to realise that cyber attacks can destroy or change huge amounts of accounting, trading and payment information. It is crucial that the management knows what is going on should a cyber attack take place. It must be able to communicate what has happened to the rest of the world and to plan how the firm would restore its systems afterwards.

In the last couple of months, important figures in the financial services sector have expressed their concerns about cyber crime. DTCC, the trade repository, has said that cyber crime is a very important threat, and Andy Haldane, executive director, financial stability at the Bank of England has made similar remarks. Leading regulators have also warned about cybe rcrime.

Regulators and financial institutions all have the same interests: to maintain a resilient financial system and to protect against criminals who are trying to disrupt the financial system.

The exchange of information among regulators and the markets will be essential, and that is something that is now taking place. And fortunately there is trust among them. IOSCO is helping to facilitate the dialogue because it is very important that all players understand the patterns surrounding cyber crime. It is

a very positive sign that regulators around the world are engaging with their financial institutions and with IOSCO, and all this will help us in making global principles. Politicians are also very aware of cyber risks, and hopefully sanctions regimes will then be put in place. Governments have to develop the ability to detect and pursue cyber criminals.

Some countries, such as the Netherlands, have set up cyber units as part of their military organisations, whose role is to detect and go after cyber criminals around the world. Others have recognised the importance of having resilient systems that are linked to the financial system. The financial infrastructure is critical, much like natural resources such as water. If a country's financial system is attacked, the entire system, economy and society will be hurt, and that has now been widely recognised.

- ***Patricia Lee*** *is South-East Asia editor at Compliance Complete in Singapore. She also has responsibility for covering wider G20 regulatory policy initiatives as they affect Asia.*