Bank of England issue questionnaire designed to increase cyber security

Date : August 25, 2015

The Bank of England recently wrote to insurance companies with a questionnaire designed to help the Prudential Regulation Authority (PRA) get a sense of the sector's approach to cyber security. The questionnaire also includes questions from the Financial Conduct Authority (FCA). The questionnaire is just the latest in a line of initiatives from regulators designed to increase cyber resilience.

History

The interest of financial regulators in cyber security is not new. In 2007 the Financial Services Authority (FSA) fined Nationwide Building Society £980,000 for failing to have effective systems and controls in place to manage its information security risks. In 2009 the FSA fined three HSBC firms over £3 million for not having adequate systems and controls in place to protect their customers' confidential details from being lost or stolen. The entities fined were HSBC Life UK Limited, HSBC Actuaries & Consultants Limited and HSBC Insurance Brokers Limited. Whilst most of the regulator's activity has been in response to security breaches other financial services organisations have been fined for failure to have proper procedures in place.

In addition the Bank of England have been working with HM Treasury, the FCA and others to develop CBEST, a new framework for sharing detailed threat intelligence and delivering cyber security tests and benchmarking for UK financial services providers. CBEST is the first of initiative of its type to be led by any of the world's central banks.

What is this new initiative?

The PRA questionnaire consists of three main sections:

1. Cyber security and resilience capabilities – this part of the questionnaire is designed to give an overview of the firm's policies and capabilities in relation to cyber risk.
2. Cyber insurance – the PRA is trying to collect data on the extent to which cyber insurance policies are being written.
3. Conduct – this section of the questionnaire has been developed by the FCA (in some respects the successor to the FSA) and is intended to work out the confidential customer information firms receive and how this is handled and stored.

What is the deadline?

The questionnaire has to be filled in by *"competent parties within the firm who have the appropriate knowledge and experience to be able to answer the questions in the various sections of the questionnaire"*. It then must be signed-off by a board level executive as a true and accurate reflection of the current status of cyber resilience. Questionnaires have to be returned by Friday 16 October.

Are there any concerns?

Clearly for some organisations who have not looked holistically at cyber risk there's a lot to cover. Some organisations will find it challenging to do the risk assessment required in the 10 weeks allowed with an appropriate level of confidence for the board to sign off. The questionnaire does not allow for uncertainty. Questions cannot be left blank and the PRA says *"all questions must be answered to the firm's best ability"*. The company must also be prepared to provide supporting evidence for the answers it gives.

The questionnaire comes at a time of unprecedented attacks on the financial services sector. Whilst the questions asked are open questions they suggest that the PRA have in mind a number of things that they would like regulated entities to do including:

1. Having a cyber security strategy approved by the board.
2. Making sure that senior executives understand their roles and responsibilities.
3. Providing all staff with cyber security training with additional training for higher risk staff.
4. Assessment of third party providers' security capabilities (this is important as some providers to the insurance market have suffered cyber attacks).
5. Performing regular vulnerability scanning and penetration testing.
6. Having a breach notification policy and plan in place.

For most financial services organisations having a data breach is a case of when not if particularly if they rely on third party providers and systems without doing appropriate due diligence.

What needs to be done?

Organisations receiving the questionnaire clearly need to start work now to provide the appropriate answers and evidence which will demonstrate that they are on top of cyber security issues. Businesses will want to work hard to identify any gaps and a plan to fill those gaps – for example by putting in place training programmes now. A thorough risk assessment should also be done. There's a short film here explaining some of the risks the financial services industry faces.

It is important to stress however that filling in the questionnaire cannot be the end of the process. Cyber security requires perpetual vigilance as the risks change. In addition the proposed new EU Regulation on data protection will increase the security breach reporting obligations for insurers and others (see our FAQs here). For most insurers the questionnaire should be a real indication that cyber issues are business critical and require the engagement of the board.

Cordery is experienced in cyber security matters – both in helping prevent incidents happen and in responding when a breach occurs. We're also experienced in providing state of the art information security training to financial services organisations. There are details of our cyber security practice here.

Jonathan Armstrong & Gayle McFarlane are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

Gayle McFarlane Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 118 2700