BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Andrew Bulley
Director
Life Insurance

Chris Moulder
Director
General Insurance

10 August 2015

Dear [insert]

CYBER RESILIENCE CAPABILITIES QUESTIONNAIRE

Our letter on cyber resilience in July gave advance notice to firms of a questionnaire designed to help the PRA understand firms' current policies and capabilities in this area. The questionnaire (including guidance notes) is attached and consists of three main sections:

1. **Cyber security and resilience capabilities** – the multiple choice and free text questions are designed to provide an overview of the firm's policies and capabilities in relation to cyber risk.
2. **Cyber insurance** – this is intended to collect information on the extent to which the firm is underwriting cyber insurance business, and the possibility of other lines of business to potentially be called upon to pay. Where a firm does not write any cyber specific or general insurance business (which is likely to be the case for most life insurers) this section of the questionnaire can be left blank.
3. **Conduct** – this section of the questionnaire has been developed by the Financial Conduct Authority (FCA) and is intended to ascertain what confidential customer information firms receive (in relation to both cyber-insurance products and more generally) and how this is handled and stored.

The questionnaire should be completed 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. The completed questionnaire should be signed off by a board-level executive of the relevant UK legal entity or group as a true and accurate reflection of the current status of cyber resilience, and returned to the firm's usual PRA supervisory contact by cob Friday 16 October 2015. Any queries should be addressed in the first instance to the firm's usual PRA supervisory contact.

As noted above, section 3 of the questionnaire has been developed by the FCA. Firms do not need to send the completed questionnaire to the FCA: we will share results with the FCA in due course.

Yours sincerely

Andrew Bulley **Chris Moulder**

PRA CYBER RESILIENCE/INSURANCE QUESTIONNAIRE 2015

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

PLEASE READ THE GUIDANCE NOTES SECTION BEFORE COMPLETING THE QUESTIONNAIRE

Company Name:	

Date Completed:	

Completed by:		
Role:		
Completed by:		Complete for additional personnel as required
Role:		
Completed by:		Complete for additional personnel as required
Role:		
Completed by:		Complete for additional personnel as required
Role:		
Completed by:		Complete for additional personnel as required
Role:		
Completed by:		Complete for additional personnel as required
Role:		

Executive Sign Off:		Details of Executive / Board Member confirming that the answers provided are a true and accurate account of the company's position in relation to their cyber security and resilience capabilities (as applicable to the questions posed) and their exposures to cyber-specific and non-specific insurance products (as applicable to the areas listed within the insurance supplement).
Position held:		
Date:		

PLEASE REFER TO YOUR LEAD SUPERVISOR SHOULD YOU HAVE ANY QUESTIONS ON HOW TO COMPELETE THIS QUESTIONNAIRE

Insert supervisor contact information here

QUESTIONNARE GUIDANCE NOTES

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Who should complete the questionnaire?	*The questionnaire should be completed by competent parties with appropriate IT/Cyber risk knowledgeable and experience, and are sufficiently familiar with the firm's organisation's IT/Cyber resilience operating practices and procedures.*
Who should sign-off the completed questionnaire?	*The questionnaire will need to be signed-off at board level for the UK regulated entity as a true and accurate reflection of the firm's cyber resilience capabilities.*
What do we mean by 'Cyber Resilience'?	*Traditional cyber defence strategies, such as firewalls and intrusion-detection systems, are no longer enough to prevent determined threat actors. Cyber attacks are now so numerous and sophisticated that some will inevitably get through even the most robust defensive capabilities.* ***Cyber Resilience is about the management rather than the elimination of cyber risk. It recognises that security needs go beyond systems, software or IT departments and establishes procedures and protocols for; Governance Oversight, Culture, Risk Identification, Protection, Detection, Response and Recovery.***
What do we mean by 'Effective' or 'Effectiveness' in questions 4, 5, 11a, 11b, 11c, 21b, and in answers A and C to quetsion 5, and answer A to question 24?	*Effective' and 'Effectiveness' is defined as "A high level of assurance that the proposed change(s) or action that will be implemented or has been undertaken will bring or has brought about the desired or intended result".* ***NB The firm should be prepared to provide supporting evidence for this as and when required by the PRA.***
How much of the firm should the completed questionnaire reflect?	*The questionnaire must reflect the entire UK regulated entity including any relevant group and/or external (third party) support IT/Cyber services whether these are in the UK and/or overseas that form part of the UK firm's cyber resilience capabilities.*
What is the deadline for completion/return to the PRA?	*The completed questionnaire should be returned to the PRA by no later than 10 weeks from the date the questionnaire was sent to the firm.*
Will the firm need professional support to complete the questionnaire?	*No. The questionnaire is intended to reflect the firm's own opinion of their current status of cyber resilience and should not need/involve professional support/advice.*
What amount of detail is required for free text answers?	*Please do not exceed 100 words for each free text answer.*
How should I answer if more than one answer applies?	*Select the answer that consistently applies to all regulated entities and/or service support covered by the questionnaire – 'lowest common denominator' principle applies.*
Can any questions be left blank if we are uncertain of the current position for the firm?	*No. All questions must be answered to the firm's best ability.*
Will we need to provide documentation and/or information that supports the answer selected?	*Evidence supporting each answer selected by the firm is not required by the completion deadline. Only the completed questionnaire need be returned to the PRA by the deadline. The firm should however be prepared to provide supporting evidence as and when this may be required by the PRA.*
Who should we send the completed questionnaire to?	*Due to the sensitive nature of the information provided, the completed questionnaire should only be sent a) electronically, b) to your Lead Supervisor (contact information provided on Company Information tab), and c) in an encrypted format.* ***NOTE Please contact your Lead Supervisor before sending the completed questionnaire by email to ensure they are available to receive and process the docment.***

August 2015

CYBER SECURITY AND RESILIENCE CAPABILITIES

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Company Name:	0				
	QUESTION	**SELECT ONE RESPONSE ONLY (From the right hand side drop down 'Selection')**			
		Evidence supporting each answer selected by the firm is not required by the completion deadline. Only the completed questionnaire need be returned to the PRA by the deadline. The firm should however be prepared to provide supporting evidence as and when this may be required by the PRA.			**QUESTIONNAIRE INCOMPLETE**
	GOVERNANCE & LEADERSHIP				Select one response for each question (unless a free text response has been requested). You must select one answer for each question.
		A	**B**	**C**	
1	**Has your cyber security strategy been approved by the Board?**	Yes	No, but it is being submitted for approval within 6 months	No	Selection:
2	**Do senior executives understand their roles and responsibilities?**	Yes , and their understanding has been validated	They have been informed and understanding is assumed	No	Selection:
3	**Have cyber security roles within the organisation been aligned to the strategy? (you MUST answer no, if you answered No to Q1)**	Yes	No, but this is in progress and will be aligned within 6 months	No, it is assumed existing cyber security roles are sufficient	Selection:
	IDENTIFY				
		A	**B**	**C**	
4	**Are effective risk management practices in place to address cyber security risks?**	Yes, and these are well documented and understood	Not specifically, but existing operational risk practices have been deemed appropriate	No, it is assumed that existing practices are sufficient	Selection:
5	**For whichever response to Q4, do you measure the effectiveness of the implementation of these practices?**	Yes, and effectiveness is regularly included in MI reporting	Yes, it is measured, but not reported or challenged	No, it is assumed that they are implemented effectively	Selection:
6	**Do you have a process to identify your organisation's critical functions and processes?**	Yes, and this is annually verified	Yes, this activity has been undertaken but it is not considered a routine, repeatable process	No	Selection:
6a	**Please describe this process, include and how critical functions are defined?**				
7	**Has all IT supporting the delivery of those critical functions and processes been identified? (you MUST answer no, if you answered no to Q6)**	Yes, and this is annually verified	Yes, this activity was undertaken but has not been repeated recently	No, all IT is considered critical	Selection:
8	**Has sensitivity and integrity of the data required for the delivery of critical functions been assessed? (you MUST answer no, if you answered no to Q6)**	Yes, and this is annually verified	Yes, this activity was undertaken but has not been repeated recently	No, all data is considered sensitive	Selection:
9	**Are hardware and software vulnerabilities identified, documented and remediated?**	Yes, and there is an established process for prioritisation of critical vulnerabilities	Yes	No, vulnerabilities are remediated on an ad-hoc basis	Selection:
10	**Are your protection activities informed through the use of threat information?**	Yes, we process multiple sources and produce our own threat intelligence	Yes, we receive threat information from third party vendor(s)	No	Selection:
	PROTECT				
		A	**B**	**C**	
11a	**Are effective physical access controls implemented, maintained and monitored across your organisation's facilities?**	Yes, and these are reviewed on an regular basis	Yes, there are controls in place, but there is no routine review process	There are some, but I can not be sure that they are implemented across the organisation, or No.	Selection:
11b	**Are effective remote access controls implemented, maintained and monitored across your organisation's facilities?**	Yes, and these are reviewed on an regular basis	Yes, there are controls in place, but there is no routine review process	There are some, but I can not be sure that they are implemented across the organisation, or No.	Selection:
11c	**Are effective privileged user access rights implemented, maintained and monitored across your organisation's facilities?**	Yes, and these are reviewed on an regular basis	Yes, there are controls in place, but there is no routine review process	There are some, but I can not be sure that they are implemented across the organisation, or No.	Selection:
12	**Are all staff provided with cyber security training?**	Yes, and MI is collected on completion of training	Yes, training is made available to all staff, no MI is collected	No, training is ad-hoc	Selection:
13	**Is additional training provided to higher risk staff?**	Yes, and MI is collected on completion of training	Yes, training is made available to all staff, no MI is collected	No, they only receive the same training as per the response to 12	Selection:
13a	**If you answered Yes to 13, please define 'higher risk staff'**				
14	**Which option best describes your data loss prevention strategy?**	Full, and documented strategy and process	Partial, and aligned to critical systems and data only	None in place	Selection:
14b	**What monitoring and tools are used?**				
15	**Which option best describes how data is stored?**	All data is encrypted at rest	All data considered critical is encrypted at rest	No data is encrypted at rest	Selection:
16	**Which option best describes your data back-up process?**	All data is backed up, multiple formats	Critical data is backed up, multiple formats	Some data is backed up, single format	Selection:
16b	**Describe how frequently you undertake back ups and also describe how you test the data to ensure that the back ups are fit-for-purpose**				
17	**How do you assess third-party providers' security capabilities?**	Conduct audit of third party	Self-certification	No assessment conducted	Selection:
17a	**How often are these assessment carried out?**	Bi-annually	Annually	Less then annually	Selection:
	DETECT				
		A	**B**	**C**	
18	**Have you produced and maintained a baseline of network operations and expected data flows?**	Yes, and this is annually reviewed and verified	Yes, we undertook this process but a review has not taken place	No	Selection:
19	**Which option best describes your network detection and monitoring processes and controls?**	All events are analysed (automated and manual) to attribute attacker, methodology and potential impacts to critical functions and processes	An automated system highlights anomalies but little analysis is undertaken	No capability to analyse network anomalies	Selection:
20	**Do you perform regular vulnerability scanning?**	Yes, we have a rolling programme, agreed at Board (or Senior Executives) level	Yes, there is a regular programme in place	No, vulnerability scanning is performed on an ad-hoc basis	Selection:
21	**Do you perform regular penetration testing?**	Yes, we have a rolling programme, agreed at Board (or Senior Executives) level	Yes, there is a regular programme in place	No, penetration testing is conducted on an ad-hoc basis	Selection:
21b	**Describe how frequently you undertake vulnerability scanning and penetration testing and ensure that both are effective.**	Yes - more than monthly	Yes - between annually to monthly	No we do not	Selection:
	RESPOND & RECOVER				
		A	**B**	**C**	
22	**Are thresholds (aligned to impacts) set for events and incidents to determine appropriate response?**	Yes and these have been approved by business and supporting IT functions	Yes and these have been approved by supporting IT functions	No formal thresholds, we respond on an ad-hoc basis	Selection:
23	**Do you buy cyber insurance?**	Yes, we buy cyber-specific insurance	Yes, this is included within our general property and liability insurances	No	Selection:
24	**Do you have a documented and regularly tested response plan (Business continuity, disaster recovery and/or cyber incident response)?**	Yes. We have separate cyber incident response, disaster recovery and business continuity plans forming a recovery framework. The effectiveness of this framework has been tested in the last 12 months	Yes. We have separate cyber incident response, disaster recovery and business continuity plans. These have been tested separately within the last 12 months and it is assumed that they can work collectively.	Existing business continuity plans are considered sufficient, but these have not been tested against a cyber incident	Selection:
25	**Describe your data breach notification policy?**	All critical breaches are to be reported to: Law enforcement, customers and regulator	Critical breaches are reported internally only	No formal breach notification policy	Selection:
25a	**Define what you consider a critical data breach**				
26	**Is voluntary information sharing included within the response plan (do not answer if you responded No to 22)**	Yes, this is expected and sharing requirements are clearly set out	Yes, information sharing is undertaken as appropriate with specifics being determined following an event	No	Selection:
27	**In addition to any analysis referred to in the Detect Section, do you undertake forensic activities following events and incidents?**	Yes, we conduct internal forensic analysis which is supported by specialist third parties	Yes, forensic analysis is conducted internally or; by a specialist third party	No	Selection:
28	**Does your response planning (as discussed in 22) explicitly refer to recovery activities, including retuning to normal operations, or to a pre-defined, acceptable level?**	Yes, and the timeframe for returning to normal operation / acceptable level is reviewed on an annual basis.	Yes, but the timeframe for returning to normal operation / acceptable level has not been reviewed in the last 12 months	No	Selection:

August 2015

FOR PRA USE ONLY

TOTALS	A	0
	B	0
	C	0
TOTAL		0

QUESTIONNAIRE INCOMPLETE

CYBER INSURANCE SUPPLEMENT

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Company Name:	0

August 2015

1. If the reporting company issued any specific cyber insurance products in the calendar year 2014, please provide the following:

Direct Premiums		First Party Direct Losses		Third Party Direct Losses		Number of Policies in Force	
Gross Written £000's	Gross Earned £000's	Paid £000's	Outstanding £000's	Paid £000's	Outstanding £000's	Claims Made	Occurrence

What is the range of limits issued in the specific cyber insurance products: (min) _____ to (max) _____

2. For all other non-cyber specific insurance policies issued, please provide the following:

Answering YES or NO, in which of the following lines of business has a cyber exclusion clause (such as CL380, NMA 2419 or similar) been included consistently on all

	YES	NO	If **NO**, please provide estimated annual Gross Earned Premium for portfolio where no cyber exclusion clause has been included in the policy: 2012	2013	2014	Indicate if portfolio has predominantly claims-made (**CM**) or occurrence (**OCC**) claims trigger
Commercial Property						
Commercial Consequential Loss						
Commercial Motor						
Commercial Public and Products Liability						
Commercial Employers Liability						
Commercial Contractors and Engineering risks						
Commercial Professional Liability						
Commercial Mixed Packages						
Commercial Fidelity and Contract Guarantee						
Commercial Credit						
Commercial Surety						
Aviation Liability						
Aviation Hull						
Space and Satellite						
Marine Liability						
Marine Hull						
Marine Cargo						
Energy (Onshore & Offshore)						
Protection and Indemnity						
Transport War Risks						
Goods in Transit						
Personal Motor						
Personal Household						
Personal Accident & Sickness						
Personal Travel						
Personal Extended Warranty						
Personal Legal Expenses						

NOTES:

- Cyber Insurance products is defined as coverage in part or whole for first party and/or third party costs/damages arising out of unauthorised use of, or unauthorised access to, electronic data or software within the
- Direct premiums, losses and defence/cost containment expenses for cyber specific insurance products are to be reported before reinsurance
- Direct premiums, losses and defence/cost containment expenses for cyber specific insurance products are to be reported before reinsurance

Additional informational/Explanation provide by the Company (optional):

CYBER RESILIENCE QUESTIONNAIRE - FCA ADDITIONAL QUESTIONS

Company Name	0

Please return these questions with the main questionnaire to your PRA supervisor, who will in turn share both questionnaires with the FCA over secure links.

1. If the reporting company issues any specific cyber insurance products, please answer the following questions:

What information is required from clients during the underwriting process in order to underwrite these products? *NOTE: We will accept copies of proposal forms in response to this question, if appropriate.*	
Which business areas receive this information and have access to it, and for how long is the information retained?	
Once received, how is this information stored, how is it secured and if encrypted to what standard is it encrypted?	

What expertise does the reporting company use to interpret this information?	A	B	C	SELECTION
	In-house experts who maintain information security or cyber security qualifications	Existing staff within the underwriting department	Outsourced cyber expertise	

1a.		
	If the answer to the above question is C, please detail to whom this activity is outsourced.	

2. Across all products sold:

How is consumer Personally Identifiable Information (PII) classified, how long is this data retained, how is it secured, if encrypted once stored then to what standard is it encrypted?	

3. Across all products sold:

How is confidential customer information (such as Bank Account or Credit / Debit card details) classified, how long is this data retained, how is it secured, if encrypted once stored then to what standard is it encrypted?	

Additional Information / Explanation provided by the reporting company (optional)