

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.
- 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



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
Position held:		company's position in relation to their cyber security and resilience capabilities (as applicable to the questions pose
Date:		and their exposures to cyber-specific and non-specific insurance products (as applicable to the areas listed within th
<u>-</u>		insurance supplement).
	PLEASE REFER TO YOUR LEAD SUPERVISOR SHOULD	YOU HAVE ANY QUESTIONS ON HOW TO COMPELETE THIS QUESTIONNAIRE
	Insert sup	pervisor contact information here

QUESTIONNARE GUIDANCE NOTES



Who should complete the questionnaire?

Who should sign-off the completed questionnaire?

What do we mean by 'Cyber Resilience'?

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?

How much of the firm should the completed questionnaire reflect?

What is the deadline for completion/return to the PRA?

Will the firm need professional support to complete the

What amount of detail is required for free text answers?

How should I answer if more than one answer applies?

Can any questions be left blank if we are uncertain of the current position for the firm?

Will we need to provide documentation and/or information that supports the answer selected?

Who should we send the completed questionnaire to?

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.

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 resilienci capabilities.

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.

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.

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.

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.

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.

Please do not exceed 100 words for each free text answer.

Select the answer that consistently applies to all regulated entities and/or service support covered by the questionnaire — 'lowest common denominator' principle applies.

No. All questions must be answered to the firm's best ability.

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

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 Superviso before sending the completed questionnaire by email to ensure they are available to receive and process the docment.

August 2015



Martin M						
Montanger Mont	Com	pany Name:	0			
Application		QUESTION				
Section Control Cont	Г		Evidence supporting each answer selected by the firm i	s not required by the completion deadline. Only the comp	pleted questionnaire need be returned to the PRA by the	OUESTIONINAIDE INCOMPLETE
March Company Compan					n this may be required by the PRA.	Select one response for each question (unless a
Security of the control of the contr				LEADERSHIP		
Section Sect		Has your cyber security strategy been approved by the	A	No, but it is being submitted for approval within 6	С	select one answer for each question.
Secretary Company Co	1	Board?	Yes	months	No	Selection:
The content of the	١,	Do senior executives understand their roles and responsibilities?	Yes , and their understanding has been validated		No.	Selection:
Section Part			res, and their direct stationing has been variabled	assumed		Section.
Company Comp			W			e de arte e
A particular discrepancy of proteins in plane in the company of th	3	you answered No to Q1)			sufficient	Selection:
Legislation and contract models of the contra			IDENTI	FY		
Septiment and control to the control			A	В	С	
The production of the control of the						
Section of the empherostation of the sequence of the control of th	4		Yes, and these are well documented and understood	have been deemed appropriate	No, it is assumed that existing practices are sufficient	Selection:
Services and programment commony and appropriate for the common programment of the common progra			Yes, and effectiveness is regularly included in MI		No, it is assumed that they are implemented	
Section of the content of the cont			reporting	Yes, it is measured, but not reported or challenged	effectively	Selection:
The formation of services and experimental to the control of the c			Yes, and this is annually verified		No	Selection:
Set of the control of						
According any agreement was the application of the control of th						
See an extraction of the control of		functions and processes been identified? (you MUST				
Mark Control of the Control of t	7	answer no, if you answered no to Q6)	Yes, and this is annually verified	repeated recently	No, all IT is considered critical	Selection:
Math Continued Math Continued Math		Has sensitivity and integrity of the data required for				
Management and continuous activations activated by the continuous activation of the continuous activa		the delivery of critical functions been assessed? (you	Voc. and this is approally use for t		No. all data is someidered as 1.77	Caladian
March Control Contro	8			repeated recently	ivo, an uata is considered sensitive	selection:
The set of the set o	9	documented and remediated?	prioritisation of critical vulnerabilities		No, vulnerabilities are remediated on an ad-hoc basis	Selection:
See deficient physical according injunctional control of the contr	\Box				No.	Selection
The Process of Section of Property and Section of Process of Section of Secti	10	use or un'edt illioriildtions		11	INO	Sciection.
Less designation of the control of t			PROTE	СТ		
The control of the co			A	В	c	
La facilità de mainte au respectation proposed de la completación de l	П			Yes, there are controls in place, but there is no routine	There are some, but I can not be sure that they are	
Lange Marketine of the control and control	11a	facilities?	Yes, and these are reviewed on an regular basis			Selection:
The place of the color of the				Ves there are controls in place but there is no as	There are some but I can not be core that they core	
International professional control professional processors of the control processors of the cont	11ь	mamameu and monitored across your organisation's facilities?	Yes, and these are reviewed on an regular basis			Selection:
The production function function function function function of the part of t	F	Are effective privileged user access rights		`		
A set al stell provided with regions to provide the large or day and the collected on completion of travering the collected of completion of travering the collected of completion of travering the collected of completion of travering collected on completion of travering collected or completion or completion or control of collected or completion or com	L		Yes and these are reviewed on an regular hasis			Selection:
20 Ambility of transported that the place security framings 10 Ambility of transported in bulber of salt for salt fo			and the second of an regular basis		mental delays the organisation, or no.	
gill seed for the control of the c	12	Are all staff provided with cyber security training?	Yes, and MI is collected on completion of training	collected		Selection:
The second from the 1-big price of the Telephoritics of the Second Control of the Second	12	Is additional training provided to higher risk staff?	Yes, and MI is collected on completion of training			Selection:
The content of the						· · ·
In contact Part An executable of the color of the c	13a	staff'				
150 What monitoring and tools are used? 150 What monitoring and tools are used? 150 What monitoring produced are used? 150 What monitoring receives your desirable what size server? 150 What monitoring receives your desirable what size server? 150 What monitoring receives your desirable what size server? 150 What monitoring receives your make that we saw and your make that we have the transport of the proper what is nown to be the proper what is nown to			Full, and documented strategy and process	Partial, and aligned to critical systems and data only	None in place	Selection:
12 to the part earlier teaching trave and in stanced? 13 process? 14 process? 15 process? 16 process? 16 process? 16 process? 17 process? 18 process? 19 process? 19 process? 19 process? 10 process?				· · · · · · · · · · · · · · · · · · ·		
Whether processes was described, by our produced and maintained a baseline of the processes and centroling. Whether programs was also described to the post of the season must the baseline of the processes and centroling. The processes and centroling of the processes and centroling of the processes and centroling of the processes and centroling. The processes and centroling of the processes and centroling of the processes and centroling of the processes and centroling. The processes and centroling of the processes and centroling of the processes and centroling of the processes and centroling. The processes and centroling of the processes and centroling of the processes and centroling of the processes and centroling. The processes and centroling of the processes and centroling of the processes and centroling of the processes and centroling. The processes and centroling of the proces						
Lange Description for responsity you understable back day and all and backed up, multiple formats on the proper of the proper sets the data to ensure the betty and the proper of the pr			All data is encrypted at rest	All data considered critical is encrypted at rest	No data is encrypted at rest	Selection:
Do spoul price marked and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained as baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced and maintained a baseline of 1/2 interests of spoul produced spoul produced spoul produced by spoul produced			All data is backed up, multiple formats	Critical data is backed up, multiple formats	Some data is backed up, single format	Selection:
As the control for your test the data to resure that the back up are affective for your purpose. See for the first the firs	_					1
In the case of your autests third party providers' according one? Now often are these assessment carried out? Section		also describe how you test the data to ensure that the				
New Year are these assessment carried out? But annually Less then annually Selections	16b	back ups are fit-for-purpose How do you assess third-party providers' security				
A Section for the describe your network detection for the describe your perform regular understillity scanning? 20 Do you perform regular penetration testing? 21 Do you perform regular penetration testing and ensure that your describe your describe your describe your describe your described your de			Conduct audit of third party	Self-certification	No assessment conducted	Selection:
A Section for the describe your network detection for the describe your perform regular understillity scanning? 20 Do you perform regular penetration testing? 21 Do you perform regular penetration testing and ensure that your describe your describe your describe your describe your described your de	17.	How often are these assessment carried out?	Bi-annually	Annually	Less then annually	Selection:
A set thresholds (aligned to impact) as for event and respected and regularly resistive that the should (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls? B Oy you perform regular programme (agreed all floors) for event and processes and controls? A set thresholds (aligned to impact) as for event and processes and controls) while the programme (agreed all floors) for event and processes and controls? B Oy you but y city important to return appropriate response? D Oy you have a documented and regularly tested T vs., we have separate cyber incident response, disaster recovery and business continuity plans are considered within the processes and processes and controls? A set thresholds (aligned to impact) set for event and processes a	1/a					
In the your produced and maintained a baseline of performed and verified processes and expected data flowers? Which option best describes your network detection to grow many processes and controls? Which option best describes your network detection to grow many processes and controls? Which option best describes your network detection to grow many processes and controls? Perform regular vulnerability scanning: Perform regular vulnerabilit			DETEC	-		
10 New control protections and expected data flows? Ves. and this is annually reviewed and verified by the price of the describes your network detection All reviewed and verified programme, agreed at loard (or 20 Ves., we have a rolling programme, agreed at loard (or 20 Ves., where is a regular programme in place No. capability to analyze network anomalies Selection No. capability to analyze network a			A	В	с	
Mich option bet describes your network detection 19 and monally to monitoring processes and controls? Which option bet describes your network detection 19 and monitoring processes and controls? Do you perform regular vulnerability varaning? No we perform regular vulnerability varaning? No we have a rolling regorgemme, agreed at Board for Senior Executives) level Senior Executives level Senior Executives (senior Executives) level Senior (senior Executives) level Senior Executives (senior Executive			Yes, and this is annually reviewed and verified		No	Selection:
Which option best describes your network detection attribute attacker, methodology and potential impacts a pand monitoring processes and corrective? 20 Jo you perform regular vulnerability scanning? 21 Do you perform regular ponetration testing? 22 Do you perform regular penetration testing? 23 Do you perform regular penetration testing? 24 Do you perform regular penetration testing? 25 Do you perform regular penetration testing? 26 Do you perform regular penetration testing? 27 Do you perform regular penetration testing? 28 Do you perform regular penetration testing? 29 Do you perform regular penetration testing? 20 Do you perform regular penetration testing? 21 Do you perform regular penetration testing and ensure that yes in monthly 22 Do you perform regular penetration testing and ensure that yes in monthly 23 Do you perform regular penetration testing and ensure that yes in monthly 24 Part Persenolds (pilipped to impacts) set for events and you penetral penetration testing and ensure that yes in monthly 25 Do you buy open insurance? 26 Do you have a documented and regularly tested exponse plan (so hours and yes in monthly plans are considered and regularly tested with the penal p	18			proce.		
Ves. we have a rolling programme, agreed at Board (or least the position Executives) level vous perform regular vulnerability scanning? 20 by operform regular programme, agreed at Board (or least the position Executives) level vous perform regular programme, agreed at Board (or least the position Executives) level vous undertake vulnerability scanning and penstration testing? 21 by operform regular programme, agreed at Board (or least the position Executives) level vous undertake vulnerability scanning and penstration testing and ensure that vous undertake vulnerability scanning and penstration testing and ensure that vous undertake vulnerability scanning and penstration testing and ensure that vous undertake vulnerability scanning and penstration testing and ensure that vous undertake vulnerability scanning is performed on an ad-hoc basis selection: **RESPOND & RECOVER*** **Ps. where is a regular programme in place basis on the position position of the position position of the position position of the position position to determine appropriate response?* 20 by our bury of ever insurance?** 21 by our bury of ever insurance?** 22 by our bury of ever insurance?** 23 by our bury of ever insurance?** 24 very have a documented and regularly tested desprease pain fluidings continuity, disaster recovery and business continuity plans of the form that they can work collectively.** 25 by office what you consider a critical data breach to the less 12 months are possible pos			attribute attacker, methodology and potential impacts		No constitute and	Saladian
20 Do you perform regular unknability scanning of you perform regular penetration testings of programme, agreed at Board (or possible and possible a	19	and monitoring processes and controls?		anaiysis is undertaken		Selection:
Do you perform regular penetration testing? Semior Executives) level Ves. there is a regular programme in place Dasis Selection:	20	Do you perform regular vulnerability scanning?	Senior Executives) level	Yes, there is a regular programme in place	basis	Selection:
Describe how frequently you undertake vulnerability scanning and penetration testing and ensure that Ves. more than monthly Ves. between annually to monthly No we do not Selection: Page						Salaction
se-more than monthly Yes - between annually to monthly No we do not Selection: Selection: Select			Demoi executives) level	Yes, there is a regular programme in place	Dasis	selection:
RESPOND & RECOVER A Re thresholds (aligned to impacts) set for events and 22 incidents to determine appropriate response? A Ne thresholds (aligned to impacts) set for events and 22 incidents to determine appropriate response? A Ves and these have been approved by business and 32 incidents to determine appropriate response? Do you buy cyber insurance? Ves, we buy cyber-specific insurance Ves, We have separate cyber incident response, disaster recovery and business continuity plans are considered and regularly tested response plan (Business continuity, disaster recovery and business continuity plans are considered on this framework has been tested in the last 12 months and it is assumed that they can work collectively. A Company to the destination policy? So befine what you consider a critical data breach is soultrary information sharing included within the response plan (do not answer if you responded No to 26 22) In addition to any analysis referred to in the Detect Section, do you undertake forensic activities following 27 events and incidents? Does your response plan (an ont answer if you responded No to 28 22 22 events and incidents? Baddition to any analysis referred to in the Detect Section, do you undertake forensic activities following creturing to normal operation, or to a pre-defined, operation of acceptable level is reviewed on an annual basis. Disconting the response plan (an ont answer if you responded No to 28 22 22 events and incidents? Disconting the response plan (an ont answer if you responded No to 28 22 22 events and incidents? Provided the response plan (an ont answer if you responded No to 28 22 22 events and incidents? Provided the response plan (an ont answer if you responded No to 28 22 22 events and incidents? Provided the response plan (an ont answer if you responded No to 28 22 22 22 events and incidents? Provided the response plan (an ont answer if you responded No to 28 22 22 22 22 22 22 22 22 22 22 22 22		scanning and penetration testing and ensure that			L	L
Are thresholds (aligned to impacts) set for events and 22 incidents to determine appropriate response? 20 Do you buy cyber insurance? 21 Ves, we buy cyber-specific insurance 22 Oo you have a documented and regularly tested response plan (Business continuity, disaster recovery and business continuity, disaster recovery and business continuity, disaster recovery and business continuity plans. These forming a recovery framework. The effectiveness of this framework has been tested in the last 12 months and it is assumed that they can work collectively. 25 Describe your data breach notification policy? 26 Define what you consider a critical data breach is voluntary information sharing included within the response plan (do not answer if you responded No to 26 22) 26 Define what you consider a critical data breach is voluntary information sharing included within the response plan (do not answer if you responded No to 26 22) 27 Events and incidents? 28 Define what you consider a critical data breach is voluntary information sharing included within the response plan (do not answer if you responded No to 26 22) 28 Define what you consider a critical data breach is voluntary information sharing is undertaken as appropriate with specifics being determined following an event visable provided with the continuity plans are considered sufficient, but these have not been tested against a critical breaches are reported internally only No formal breach notification policy 28 Define what you consider a critical data breach is voluntary information sharing is undertaken as appropriate with specifics being determined following an event visable provided within the response plan (do not answer if you responded Not to 26 22) 29 Define what you consider a critical data breach is voluntary information sharing is undertaken as appropriate with specifics being determined followi	21b	DOTA are effective.	res - more than monthly	res - petween annually to monthly	No we do not	Selection:
Are thresholds (aligned to impacts) set for events and 22 incidents to determine appropriate response? No formal thresholds, we respond on an ad-hoc basis selection: Yes, we buy cyber-specific insurance Ves, we buy cyber-specific insurance Yes, we have separate cyber incident response, diaster recovery and business continuity plans. The effectiveness of this framework has been tested in the last 12 months and its assumed that they can work collectively. All critical breaches are to be reported to Law enforcement, customers and regulator Selection: Yes, we have separate cyber incident response, diaster recovery and business continuity plans. These flavore special state in the last 12 months and its assumed that they can work collectively. All critical breaches are to be reported to Law enforcement, customers and regulator Selection: Yes, we have separate cyber incident response, diaster recovery and business continuity plans. These flavore special state recovery and business continuity plans are considered sufficient, but these have not been tested against a collection. Yes been sponse plan (above this this separate) within the response plan (do not answer if you responsed to 18 to			RESPOND &	RECOVER		
22 Do you buy cyber insurance? 23 Do you have a documented and regularly tested response plan (Business continuity, diasater recovery and business continuity plans are considered shave bene tested against a forming a recovery framework. The effectiveness of this is assumed that they can work collectively. 25 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification any analysis referred to in the Detect Sciencia, do you undertake forensis activities following a event and indidents? 27 events and incidents? 28 Describe your data breach notification policy? 29 Events and incidents? 20 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Events and incided within the response plan (do not answer if you responded No to your prepared to Law your consider a critical data breach so you undertake forensis activities following an event of learning included within the easy not your considers are the propertied to Law your considers are the policy of the properties to Law your considers are the propertied to Law your considers are reported to Law your considers are reported in Law your considers are reported in Law your considers are reported to Law your considers are rep			A	В	С	
22 Do you buy cyber insurance? 23 Do you have a documented and regularly tested response plan (Business continuity, diasater recovery and business continuity plans are considered shave bene tested against a forming a recovery framework. The effectiveness of this is assumed that they can work collectively. 25 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification any analysis referred to in the Detect Sciencia, do you undertake forensis activities following a event and indidents? 27 events and incidents? 28 Describe your data breach notification policy? 29 Events and incidents? 20 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Events and incided within the response plan (do not answer if you responded No to your prepared to Law your consider a critical data breach so you undertake forensis activities following an event of learning included within the easy not your considers are the propertied to Law your considers are the policy of the properties to Law your considers are the propertied to Law your considers are reported to Law your considers are reported in Law your considers are reported in Law your considers are reported to Law your considers are rep		Are thresholds (aligned to impacts) set for events and	Yes and these have been approved by business and	Yes and these have been approved by supporting IT		
25 Do you have a documented and regularly tested response plan (Business continuity, disaster recovery and business continuity plans are considered shave bene tested in the last 12 months and it is assumed that they can work collectively. 25 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Describe your data breach notification policy? 28 Describe your data breach notification policy? 29 Describe your data breach notification policy? 20 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 23 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe what you consider a critical data breach save bene tested in the last 12 months and it is assumed that they can work collectively. 25 Describe your data breach notification policy? 26 Describe what you consider a critical data breach save propriet do Law with seponse plan (do not answer if your responsed blan (an ont answer if your responsed blan (an ont answer if your responsed blan (an ont answer if your response plan (do not answer if your responsed blan (an ont an yanalysis referred to in the Detect Section, do you undertake forensic activities following an event with your described plan (an ontal and your described blan (an ontal and your described blan (an ontal your descri	22	incidents to determine appropriate response?		functions	No formal thresholds, we respond on an ad-hoc basis	Selection:
Do you have a documented and regularly tested response plan (Business continuity, disaster recovery and business continuity plans are considered approached in the last 12 months and regularly tested response plan (Business continuity, disaster recovery and business continuity plans are considered share been tested on the last 12 months and it is assumed that they can work collectively. 25 Describe your data breach notification policy? 26 Define what you consider a critical data breach is voluntary information sharing included within the response plan (Business continuity plans are considered share been tested on the last 12 months and it is assumed that they can work collectively. 27 Describe your data breach notification policy? 28 Define what you consider a critical data breach is voluntary information sharing included within the response plan (Business continuity plans are considered surflicient, but these have not been tested against a cyber incident surflicient, but these have not been tested against a cyber incident surflicient, but these have not been tested against a cyber incident response, disaster recovery and business continuity plans are considered surflicient, but these have not been tested against a cyber incident response, disaster recovery and business continuity plans are considered surflicient, but these have not been tested against a cyber incident response, disaster recovery and business continuity plans. These this framework has been tested on the last 12 months and it is assumed that they can work collectively. 28 Critical breaches are reported internally only 29 No formal breach notification policy 20 Selection: 20 Ves., information sharing is undertaken as appropriate with specifics being determined following an event with parties 20 Ves, but the timeframe for returning to normal operation, or to a pre-defined, basis. 21 Ves,	П	Do you have cahor incorposa	Voc. wo how cubor exactly income		No	Salaction
Do you have a documented and regularly tested response plan (Business continuity, disaster recovery and business continuity plans are considered forming a recovery framework. The effectiveness of this framework has been tested in the last 12 months and it is assumed that they can work collectively. 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Describe your data breach notification policy? 28 Describe your data breach notification policy? 29 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 23 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Describe your data breach notification policy? 28 Describe your data breach notification policy? 29 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 23 Describe your data breach notification policy? 24 Describe your data breach notification policy? 25 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Selection: 28 Describe your data breach notification policy? 29 Jestificatly defined within the various ponder with policy in your data breach notification policy? 29 Jestificatly defined within the various ponder with policy in your data breach notification p	23	Do you day cyper insurance?	res, we duy cyber-specific insurance	mapinity insurances	ivo	Selection.
response plan (Business continuity, disaster recovery framework. The effectiveness of his framework has been tested in the last 12 months and it is assumed that they can work collectively. 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Describe your data breach notification policy? 28 Describe your data breach notification policy? 28 Describe your data breach notification policy? 29 Describe your data breach notification policy? 29 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 23 Describe your data breach notification policy? 24 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Describe your data breach notification policy? 28 Describe your data breach notification policy? 29 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 23 Describe your data breach notification policy? 24 Describe your dat				Yes. We have separate cyber incident response,	L	
25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Describe your data breach notification policy? 28 Describe your data breach notification policy? 28 Describe your data breach notification policy? 29 Describe your data breach notification policy? 29 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 23 Describe your data breach notification policy? 24 Describe your data breach notification policy? 25 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Describe your data breach notification policy? 28 Describe your data breach notification policy? 28 Describe your data breach notification policy? 29 Describe your data breach notification policy? 29 Describe your data breach notification policy? 20 Describe your data breach notification policy? 21 Describe your data breach notification policy? 22 Describe your data breach notification policy? 22 Describe your data breach notification policy? 23 Describe your data breach notification policy? 24 Selection: 25 Describe your data breach notification policy? 25 Describe your data breach notification policy? 26 Describe your data breach notification policy? 26 Describe your data breach notification policy? 27 Selection: 28 Describe your data breach notification policy? 29 Selection: 29 Describe						
25 Define what you consider a critical data breach soft final formation sharing is undertaken as appropriat soft to any analysis referred to in the Detect Section, do you undertake forensic activities following requirements are unable to a sypon analysis referred to in the Detect Section, do you undertake forensic activities following requirements are unable to a sypon analysis referred to in the Detect Section, do you undertake forensic activities following requirements are unable to a sypon analysis referred to in the Detect Section, do you undertake forensic activities following requirements are unable to a sypon analysis in the dearly set out of the dearly set of the dearly set out of the dearly set of the dearly s			this framework has been tested in the last 12 months			Selection:
25a Define what you consider a critical data breach is voluntary information sharing included within the response plan (do not answer if you responded No to 26 22) In addition to any analysis referred to in the Detect Section, do you undertake forensic activities following: 27 events and incidents? 28 explicitly refer to recovery activities, including returning to normal operations, or to a pre-defined, operation of acceptable level is reviewed on an annual pasts. 28 acceptable level? 29 events and normal operations, or to a pre-defined, operation of acceptable level is reviewed on an annual pasts. 29 events and normal operations, or to a pre-defined, operation of acceptable level is reviewed on an annual pasts. 29 events and normal operations, or to a pre-defined, operation of acceptable level is reviewed on an annual pasts. 29 events and normal operations, or to a pre-defined, operation of acceptable level is reviewed on an annual operation of acceptable level is reviewed on an	П	Describe your data breach antifered and a 2			No formal broach notification policy	Salaction
Is voluntary information sharing included within the response plan (a not answer if you responded No to Yes, this is expected and sharing requirements are clearly set out (learly set out with specifics being determined following an event in addition to any analysis referred to in the Detect Section, do you undertake forensic activities following (learly set out section, do you undertake forensic activities following (learly set out section, do you undertake forensic activities following (learly set out set of the proposed planning (as discussed in 22) explicitly refer to recovery activities, including retuning to normal operation, or to a pre-defined, 28 occeptable level? Section, the last 12 months of the last 12 mo	25	Describe your data preach notification policy?	emorcement, customers and regulator	Critical breaches are reported internally only	NO IOITHAL Dreach notification policy	selection:
response plan (do not answer if you responded No to Zelection: In addition to any analysis referred to in the Detect Section, do you undertake forensic activities following: 27 events and indidents? Does your response planning (as discussed in ZJ) explicitly refer to recovery activities, including returning to normal operations, or to a pre-defined, operation / acceptable level? Next on the timeframe for returning to normal operations, or to a pre-defined, operation / acceptable level is reviewed on an annual basis. Yes, information sharing is undertaken as appropriate with specifics being determined following an event No Yes, forensic analysis sic conducted internally or; by a specialist third party Yes, but the timeframe for returning to normal operation, or to a pre-defined, 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 list 12 months No Selection: No Selection:	25a	Define what you consider a critical data breach				
26 22 clearly set out with specifics being determined following an event No Selection: In addition to any analysis referred to in the Detect Section, do you undertake forensic activities following Yes, we conduct internal forensic analysis which is 29 events and incidents? Oses your response planning (as discussed in 22) esplicitly refer to recovery activities, including Yes, and the timeframe for returning to normal operation / acceptable level? No Selection:			Yes, this is expected and sharing requirements are	Yes, information sharing is undertaken as appropriate		
Section, do you undertake forensic activities following 72 events and incidents? 27 events and incidents? 32 poperate by specialist third parties 32 poperate by specialist third parties 34 poperate by specialist third parties 34 poperate by specialist third parties 34 poperate by specialist third party 34 poperate by specialist third party 35 poperate by specialist third party 36 poperate by 36 poperate	26	22)			No	Selection:
22 events and incidents? 22 events and incidents? 23 explicitly refer to recovery activities, including returning to normal operations, or to a pre-defined, operation / acceptable level is reviewed on an annual obasis. 23 exceptable level? 24 supported by specialist third parties specialist third parties specialist third party No Selection: 25 event and incidents? 26 yes, and the timeframe for returning to normal operations, or to a pre-defined, operation / acceptable level is reviewed on an annual operation / acceptable level has not been reviewed in the list 12 months No Selection: No Selection: No Selection: No Selection:			Yes, we conduct internal forensic analysis which is	Yes, forensic analysis is conducted internally on his a		
Does your response planning (as discussed in Z2) explicitly refer to recovery activities, including returning to normal operations, or to a pre-defined, particular your properties of the p	27	events and incidents?			No	Selection:
retuning to normal operations, or to a pre-defined, 28 acceptable level? Operation / acceptable level is reviewed on an annual basis. Operation / acceptable level is reviewed on an annual basis. Operation / acceptable level has not been reviewed in the last 12 months No Selection:	Н	Does your response planning (as discussed in 22)	Yes and the timeframe for returning to accord	Ves but the timeframe for returning to account		
28 acceptable level? basis. the last 12 months No Selection:		retuning to normal operations, or to a pre-defined,				
	28				No	Selection:

August 2015

FOR PRA USE ONLY

TOTALS A

B

C

0

0

0

TOTAL

CYBER INSURANCE SUPPLEMENT



August 2015

Company Name: 0

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 Gross Earned		Paid	Outstanding	Paid	Outstanding	Claims Made	Occurrence
£000's	£000's	£000's	£000's	£000's	£000's		

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
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		

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 edominantly claims-made (CM) occurrence (OCC) claims trigger
<u> </u>	
<u> </u>	
_	
<u> </u>	
_	
_	
\vdash	-
\vdash	-
\vdash	
\vdash	
\vdash	
\vdash	

N	o	т	E	S	

- > 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

tional 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.

L		with the FCA over	- Secure minor		
1. I	f the reporting company issues any spec	cific cyber insurance product	s, please answer the follow	ring 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.				
Ī	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 In-house experts who maintain information security or cyber security qualifications	B Existing staff within the underwriting department	C Outsourced cyber expertise	SELECTION
	If the answer to the above question is C, please detail to whom this activity is outsourced.				
2. A	cross all products sold:				
	How is consumer Personally Identifiable Information (PII) classified, how long is this data etained, how is it secured, if encrypted once stored then to what standard is it encrypted?				
3. A	cross all products sold:				
H	How is confidential customer information (such as Bank Account or Credit/Debit card details) classified, now long is this data retained, how is it secured, if encrypted once stored then to what standard is it encrypted?				
A	dditional Information/Explanation prov	ided by the reporting compa	ny (optional)		