IAIS Consultations

Print view of your comments on "Application Paper on Supervision of Insurer Cybersecurity" - Date: 13.08.2018, Time: 18:05

Organisation	Global Federation of Insurance Associations
Jurisdiction	Global
Role	Other (not IAIS Member)
Email	secretariat@gfiainsurance.org
Phone	003228943081
Treat my comments as confidential	No

	Question
	Q1 General comments on the Application Paper
Answer	The Global Federation of Insurance Associations (GFIA) is a non-profit association established to represent national and regional insurance associations that serve the general interests of life, health, general insurance and reinsurance companies. GFIA is uniquely positioned to provide the International Association of Insurance Supervisors (IAIS) with a global perspective of global cyber risk. GFIA recognises that countries have different approaches and cultural viewpoints for addressing privacy and cybersecurity risks; however, to the extent possible, harmonisation and coordination among international governing bodies is important. GFIA's Cyber Risks working group would welcome the opportunity to have a thorough, ongoing dialogue with the IAIS on cyber risks. GFIA's global reach promotes a broad awareness of the cyber landscape and its implications for standard setters. Limiting cyber intrusions and their consequences is a shared goal of the public and private sector, and through future collaboration, GFIA believes it can help foster resilience and avoid potential unintended consequences from regulatory and standard-setting frameworks. Overall, the draft application paper is a thorough review of existing supervisory approaches to cybersecurity. Importantly, it identifies and promotes the concepts of proportionality and risk-based assessments. GFIA appreciates the effort and expertise that IAIS members and secretariat staff have put into this paper as well as the acknowledgement that there is no one-size-fits-all prescription for insurers or for supervisors. However, GFIA strongly urges caution against introducing potentially restrictive measures that may rapidly become obsolete and possibly introduce vulnerabilities due to an inflexible approach that would prevent insurers and supervisors from reacting to a rapidly changing cyber threat landscape. In particular, GFIA suggests it is inappropriate to regulate through or by prescribing/proscribing particular technologies. Technology development is fast moving and what is appropriate/inappropriate today may be obsolete tomorrow. More outcomes-focussed guidance would be appropriate as a result. GFIA respectfully recommends that the elements of proportionality and risk-based approaches be more prominently reflected in the text, particularly before every list of specific measures outlined in the application paper. GFIA is of the view that this approach would reflect the IAIS's intent, but it should be made abundantly clear that every measure in the paper is an example and not a recommended prescriptive mandate. The sections GFIA has specifically identified are examples, and GFIA would encourage you to consider this approach in every section. GFIA would also raise the issue of consistency. Use of digital technology connects to many different aspects of insurers' businesses and how the insurance business is regulated. It is therefore understandable that different IAIS working groups and/or task forces are drafting cyber/digital related standards covering different vulnerabilities the use of digital technology could create. However, this also introduces the real risk of inconsistent drafting of guidance, and highlights the importance of coordination to avoid, for example, cyber security guidance contradicting market conduct guidance (and vice versa), which cannot be

over-emphasised.

Q2 General comments on Section 1:

Answer

Q3 Comment on Paragraph 1

Answer

Q4 Comment on Paragraph 2

Answer

Q5 Comment on Paragraph 3

Answer

Q6 Comment on Paragraph 4

Answer

Q7 Comment on Paragraph 5

Answer

Q8 Comment on Paragraph 6

Answer

Q9 Comment on Paragraph 7

Answer

Q10 Comment on Paragraph 8

Answer

Q11 Comment on Paragraph 9

Answer

Q12 Comment on Paragraph 10

Answer

Q13 Comment on Paragraph 11

Answer

Q14 Comment on Paragraph 12

Answer

Q15 Comment on Paragraph 13

Answer

Q16 Comment on Paragraph 14

Answer	
	Q17 Comment on Paragraph 15
Answer	
	Q18 Comment on Paragraph 16
Answer	
	Q19 Comment on Paragraph 17
Answer	
	Q20 Comment on Paragraph 18
Answer	
	Q21 Comment on Paragraph 19
Answer	
	Q22 General comments on Section 2:
Answer	
	Q23 Comment on Paragraph 20
Answer	
	Q24 Comment on Paragraph 21
Answer	
	Q25 Comment on Paragraph 22
Answer	
	Q26 Comment on Paragraph 23
Answer	
	Q27 Comment on Paragraph 24
Answer	
	Q28 Comment on Paragraph 25
Answer	
	Q29 Comment on Paragraph 26
Answer	
	Q30 Comment on Paragraph 27
Answer	
	Q31 Comment on Paragraph 28
Answer	

	Q32 Comment on Paragraph 29
Answer	
	Q33 Comment on Paragraph 30
Answer	
	Q34 Comment on Paragraph 31
Answer	
	Q35 Comment on Paragraph 32
Answer	
	Q36 Comment on Paragraph 33
Answer	
	Q37 Comment on Paragraph 34
Answer	
	Q38 Comment on Paragraph 35
Answer	
	Q39 Comment on Paragraph 36
Answer	
	Q40 Comment on Paragraph 37
Answer	
	Q41 Comment on Paragraph 38
Answer	
	Q42 General comments on Section 3:
Answer	
	Q43 Comment on Paragraph 39
Answer	
	Q44 Comment on Paragraph 40
Answer	
	Q45 Comment on Paragraph 41
Answer	
	Q46 Comment on Paragraph 42
Answer	

Q47 Comment on Paragraph 43

Answer

Q48 Comment on Paragraph 44

Answer

Q49 Comment on Paragraph 45

Answer

Q50 Comment on Paragraph 46

Answer

Q51 Comment on Paragraph 47

Answer

Q52 Comment on Paragraph 48

Answer

GFIA supports the intent behind the concepts and considerations outlined in Paragraph 48, but would recommend preserving the concept of proportionality and risk-based assessment by changing “should” to “may” in subparagraphs a through h. Alternatively, a sentence could be added to identify that the manner in which each recommendation is implemented will depend on individual risk and proportionality calculations.

Unfortunately, the nature of the risk dictates that no entity, private or public, can be entirely secure. An entity can be expected to take only all “reasonable” measures to limit cyber intrusions and address their consequences. To that end, GFIA recommends the following amendment: “Therefore, framework objectives should aim to maintain and promote the insurer’s ability to reasonably anticipate, detect, withstand, contain, and recover from cybersecurity incidents”.

Q53 Comment on Paragraph 49

Answer

Q54 Comment on Paragraph 50

Answer

Q55 Comment on Paragraph 51

Answer

Q56 Comment on Paragraph 52

Answer

Q57 Comment on Paragraph 53

Answer

Q58 Comment on Paragraph 54

Answer

Q59 Comment on Paragraph 55

Answer

	Q60 Comment on Paragraph 56
Answer	
	Q61 Comment on Paragraph 57
Answer	
	Q62 Comment on Paragraph 58
Answer	
	Q63 Comment on Paragraph 59
Answer	
	Q64 Comment on Paragraph 60
Answer	
	Q65 Comment on Paragraph 61
Answer	
	Q66 Comment on Paragraph 62
Answer	
	Q67 Comment on Paragraph 63
Answer	
	Q68 Comment on Paragraph 64
Answer	
	Q69 Comment on Paragraph 65
Answer	
	Q70 Comment on Paragraph 66
Answer	
	Q71 Comment on Paragraph 67
Answer	
	Q72 Comment on Paragraph 68
Answer	
	Q73 Comment on Paragraph 69
Answer	
	Q74 Comment on Paragraph 70
Answer	

Q75 Comment on Paragraph 71

Answer

Q76 Comment on Paragraph 72

Answer

Q77 Comment on Paragraph 73

Answer

Q78 Comment on Paragraph 74

Answer

Q79 Comment on Paragraph 75

Answer

Q80 Comment on Paragraph 76

Answer

Q81 Comment on Paragraph 77

Answer

Q82 Comment on Paragraph 78

Answer

Q83 Comment on Paragraph 79

Answer

Q84 Comment on Paragraph 80

Answer

Q85 Comment on Paragraph 81

Answer

Respectfully, GFIA recommends aligning this section with the guidance's intent to have a risk-based and non-prescriptive approach. The Board certainly has an important role in cybersecurity oversight, but GFIA is concerned that this section may miscategorise the Board's role in some instances. For instance, where there is a recommendation for the Board "and" senior management to perform a task, "or" may be a more appropriate word choice. There is an opportunity for the application paper to clarify and distinguish between the Board and senior management. The Board must be aware of the risks and framework to manage enterprise-wide cyber risk, but senior management should establish the methodology for implementing that framework.

Similarly, in paragraph 81, subparagraph f there is a recommendation that "each insurer should designate a senior executive, such as a Chief Information Security Officer (CISO)". Requiring all insurers to have a CISO or similar position may not be possible or appropriate given the needs and resources of some insurance groups. Rather than recommending a CISO, GFIA encourages the IAIS to consider a recommendation that an employee, affiliate, or outside vendor should be responsible for implementation of the organisation's overall cybersecurity framework.

Q86 Comment on Paragraph 82

Answer

Q87 Comment on Paragraph 83

Answer

Q88 Comment on Paragraph 84

Answer

Q89 Comment on Paragraph 85

Answer

Q90 Comment on Paragraph 86

Answer

Q91 Comment on Paragraph 87

Answer

Q92 Comment on Paragraph 88

Answer

Q93 Comment on Paragraph 89

Answer

Q94 Comment on Paragraph 90

Answer

Q95 Comment on Paragraph 91

Answer

Q96 Comment on Paragraph 92

Answer

Q97 Comment on Paragraph 93

Answer

Q98 Comment on Paragraph 94

Answer

Q99 Comment on Paragraph 95

Answer

Q100 Comment on Paragraph 96

Answer

Q101 Comment on Paragraph 97

Answer

Q102 Comment on Paragraph 98

Answer

Q103 Comment on Paragraph 99

Answer

Q104 Comment on Paragraph 100

Answer

Q105 Comment on Paragraph 101

Answer

Q106 Comment on Paragraph 102

Answer

Q107 Comment on Paragraph 103

Answer

GFIA encourages the IAIS to consider qualifying language in subparagraphs m, n, and o regarding requirements to verify the security measures implemented by third-party vendors. Given the size and/or nature of the service a third-party vendor may provide, it may not be necessary or possible for an insurer to verify the cybersecurity protocols of every third-party service provider. While the security procedures of some vendors may be very important, for example a data storage vendor, not all third-party vendors provide services of a critical or sensitive nature with regard to cybersecurity.

Q108 Comment on Paragraph 104

Answer

Q109 Comment on Paragraph 105

Answer

Q110 Comment on Paragraph 106

Answer

Q111 Comment on Paragraph 107

Answer

Q112 Comment on Paragraph 108

Answer

Q113 Comment on Paragraph 109

Answer

Q114 Comment on Paragraph 110

Answer

Q115 Comment on Paragraph 111

Answer

Q116 Comment on Paragraph 112

Answer

Q117 Comment on Paragraph 113

Answer

Q118 Comment on Paragraph 114

Answer

Q119 Comment on Paragraph 115

Answer

Q120 Comment on Paragraph 116

Answer

Q121 Comment on Paragraph 117

Answer

Q122 Comment on Paragraph 118

Answer

Q123 Comment on Paragraph 119

Answer

Q124 Comment on Paragraph 120

Answer

Q125 Comment on Paragraph 121

Answer

Q126 Comment on Paragraph 122

Answer

Q127 Comment on Paragraph 123

Answer

Q128 Comment on Paragraph 124

Answer

Q129 Comment on Paragraph 125

Answer

Q130 Comment on Paragraph 126

Answer

Q131 Comment on Paragraph 127

Answer

Q132 Comment on Paragraph 128

Answer

Q133 Comment on Paragraph 129

Answer

Q134 Comment on Paragraph 130

Answer

Q135 Comment on Paragraph 131

Answer

Q136 Comment on Paragraph 132

Answer

Q137 Comment on Paragraph 133

Answer

Q138 Comment on Paragraph 134

Answer

Q139 Comment on Paragraph 135

Answer

Q140 Comment on Paragraph 136

Answer

Q141 Comment on Paragraph 137

Answer

Q142 Comment on Paragraph 138

Answer

Q143 Comment on Paragraph 139

Answer

Q144 Comment on Paragraph 140

Answer

Q145 Comment on Paragraph 141

Answer

Q146 Comment on Paragraph 142

Answer

Q147 Comment on Paragraph 143

Answer

Q148 Comment on Paragraph 144

Answer

Q149 Comment on Paragraph 145

Answer

Q150 Comment on Paragraph 146

Answer

Q151 Comment on Paragraph 147

Answer

Q152 Comment on Paragraph 148

Answer

Q153 Comment on Paragraph 149

Answer

Q154 Comment on Paragraph 150

Answer

Q155 Comment on Paragraph 151

Answer

Q156 Comment on Paragraph 152

Answer

Q157 Comment on Paragraph 153

Answer

Q158 Comment on Paragraph 154

Answer

Q159 Comment on Paragraph 155

Answer

Q160 Comment on Paragraph 156

Answer

Q161 Comment on Paragraph 157

Answer

Q162 Comment on Paragraph 158

Answer

Q163 Comment on Paragraph 159

Answer

Q164 Comment on Paragraph 160

Answer

Q165 Comment on Paragraph 161

Answer

Q166 Comment on Paragraph 162

Answer

Q167 Comment on Paragraph 163

Answer

Q168 Comment on Paragraph 164

Answer

Q169 Comment on Paragraph 165

Answer

Q170 Comment on Paragraph 166

Answer

Q171 Comment on Paragraph 167

Answer

Q172 Comment on Paragraph 168

Answer

Q173 Comment on Paragraph 169

Answer

Q174 Comment on Paragraph 170

Answer

Q175 Comment on Paragraph 171

Answer

Q176 Comment on Paragraph 172

Answer

Q177 Comment on Paragraph 173

Answer

Q178 Comment on Paragraph 174

Answer

Q179 Comment on Paragraph 175

Answer

Q180 Comment on Paragraph 176

Answer

Q181 Comment on Paragraph 177

Answer

Q182 Comment on Paragraph 178

Answer

Q183 Comment on Paragraph 179

Answer

Q184 Comment on Paragraph 180

Answer

Q185 Comment on Paragraph 181

Answer

Q186 Comment on Paragraph 182

Answer

Q187 Comment on Paragraph 183

Answer

Q188 Comment on Paragraph 184

Answer

Q189 Comment on Paragraph 185

Answer

Q190 Comment on Paragraph 186

Answer

Q191 Comment on Paragraph 187

Answer

Q192 Comment on Paragraph 188

Answer

Q193 Comment on Paragraph 189

Answer

Q194 Comment on Paragraph 190

Answer

Q195 Comment on Paragraph 191

Answer

Q196 Comment on Paragraph 192

Answer

Information sharing of threat data is an important mitigation tool that GFIA supports. However, many insurance groups have legitimate concerns about data sharing around confidentiality issues and liability. The IAIS could expand this paper to discuss more fully the role that supervisors and non-supervisory governmental bodies can play in information sharing. Sharing information should not be limited to private entities, but should also involve reciprocal sharing from supervisory and other governmental bodies. GFIA understands that some governments are interested in collaborating with industry to provide a more comprehensive threat data sharing system between all relevant parties. The IAIS could have a positive role in supporting the development of such systems on both the national and international levels, and may want to encourage governments to consider involving non-supervisory governmental bodies in information sharing arrangements. A voluntary, public-private approach, with appropriate privacy and liability protections, to sharing collective threat information can be very beneficial.

Q197 Comment on Paragraph 193

Answer

Q198 Comment on Paragraph 194

Answer

Q199 Comment on Paragraph 195

Answer

Q200 Comment on Paragraph 196

Answer

Q201 Comment on Paragraph 197

Answer

Q202 Comment on Paragraph 198

Answer

Q203 Comment on Paragraph 199

Answer

Q204 Comment on Paragraph 200

Answer

Q205 Comment on Paragraph 201

Answer

Q206 Comment on Paragraph 202

Answer

Q207 Comment on Paragraph 203

Answer

Q208 Comment on Paragraph 204

Answer

Q209 Comment on Paragraph 205

Answer

Q210 Comment on Paragraph 206

Answer

Q211 Comment on Paragraph 207

Answer

Q212 Comment on Paragraph 208

Answer

Q213 Comment on Paragraph 209

Answer

Q214 Comment on Paragraph 210

Answer

Q215 Comment on Paragraph 211

Answer

Q216 Comment on Paragraph 212

Answer

Q217 Comment on Paragraph 213

Answer

Q218 Comment on Paragraph 214

Answer

Q219 Comment on Paragraph 215

Answer

Q220 Comment on Paragraph 216

Answer

Q221 Comment on Paragraph 217

Answer

Q222 Comment on Paragraph 218

Answer

Q223 Comment on Paragraph 219

Answer

Q224 Comment on Paragraph 220

Answer

Q225 Comment on Paragraph 221

Answer

Q226 Comment on Paragraph 222

Answer

Q227 Comment on Paragraph 223

Answer

Q228 Comment on Paragraph 224

Answer

Q229 Comment on Paragraph 225

Answer

Q230 Comment on Paragraph 226

Answer

Q231 Comment on Paragraph 227

Answer

Q232 Comment on Paragraph 228

Answer

Q233 Comment on Paragraph 229

Answer

Q234 Comment on Paragraph 230

Answer

Q235 Comment on Paragraph 231

Answer

Q236 Comment on Paragraph 232

Answer

Q237 Comment on Paragraph 233

Answer

Q238 Comment on Paragraph 234

Answer

Q239 Comment on Paragraph 235

Answer

Q240 Comment on Paragraph 236

Answer

Q241 Comment on Paragraph 237

Answer

Q242 Comment on Paragraph 238

Answer

Q243 Comment on Paragraph 239

Answer

Q244 Comment on Paragraph 240

Answer

Q245 Comment on Paragraph 241

Answer

Q246 General comments on Section 4:

Answer

Q247 Comment on Paragraph 242

Answer

Q248 Comment on Paragraph 243

Answer

Q249 Comment on Paragraph 244

Answer

Q250 Comment on Paragraph 245

Answer

Q251 Comment on Paragraph 246

Answer

Q252 Comment on Paragraph 247

Answer

Q253 Comment on Paragraph 248

Answer

Q254 Comment on Paragraph 249

Answer

Q255 Comment on Paragraph 250

Answer

Q256 General comments on Section 5:

Answer

Q257 Comment on Paragraph 251

Answer

Q258 Comment on Paragraph 252

Answer

Q259 Comment on Paragraph 253

Answer

Q260 Comment on Paragraph 254

Answer

Q261 Comment on Paragraph 255

Answer

Q262 Comment on Paragraph 256

Answer

Q263 Comment on Paragraph 257

Answer

Q264 Comment on Paragraph 258

Answer

Q265 Comment on Paragraph 259

Answer

Q266 Comment on Paragraph 260

Answer

Q267 Comment on Paragraph 261

Answer

Q268 Comment on Paragraph 262

Answer

Q269 Comment on Paragraph 263

Answer

Q270 Comment on Paragraph 264

Answer

Q271 Comment on Paragraph 265

Answer

Q272 Comment on Paragraph 266

Answer

Q273 Comment on Paragraph 267

Answer

Q274 Comment on Paragraph 268

Answer

Q275 General comments on Section 6:

Answer

Q276 Comment on Paragraph 269

Answer

Q277 Comment on Paragraph 270

Answer

Q278 Comment on Paragraph 271

Answer

Q279 Comment on Paragraph 272

Answer

	Q280 Comment on Paragraph 273
Answer	