	Cyber- resilience check list			
		Current	Desired	Risk
Organisational				
1	Who in the management team is accountable to the board for information security. How do they discharge that responsibility within the organisation			High
2	Who is our data protection officer?			Medium
3	Do risk and audit committees review information security			Medium
4	Do we have relevant IT/information security policies in place, reviewed within last 2 years and **tested for compliance**			High
People				
5	Have staff been trained (certified?) on their role in effective information security - e.g. think twice before opening email attachments or clicking on links			High
6	Is downloading/installing software restricted to only authorised products/sources			High
7	Do we advise staff to separate Business and Personal. Don't use business email for personal and vice-versa			Medium
Processes				
8	Are all software patches applied quickly and out of date software eliminated			Very High
9	Have you run a penetration test within last 2 years? **Were findings acted on**			High
10	Is important data backed up regularly and kept offline and offsite			High
11	Is insurance needed/appropriate			Low
12	Do we have an action plan if we are hacked. Who does what. Budget			High
Technology				
13	Were our security systems reviewed within the last year			High
14	Do we have antivirus deployed everywhere uniformly and updated			High
15	Do we have data leakage monitoring in place (helps with theft as well)			Medium
16	Do we keep updated lists of blacklisted sites and block them			Medium
17	Do we encrypt laptops and power down in case they are stolen			High
18	Do we set standards/control what devices can connect to out network (eg Android risk)			High
19	Have IT policies been updated in last 2 years			High
20	Are all systems and components being patched regularly			Very High
	TOTAL			

Scoring

1 = Fully in place, validated annually	<25	Low risk, remain vigilant
2 = Implemented but never validated	25-50	Good progress, improve few gaps
3 = Partially planned and executed	50-70	Significant gaps to address
4 = Some actions in place, but no clear plan	>70	Very high risk, urgent action needed
5 = Not really thought about it / don't know		

Presented to the chairmens network 16/5/17 www.chairmansnetwork.com