

Assessing data quality

**Beating ‘cyber bravado’ in the NCRA questionnaire responses**

When looking at CII sector response data for the NCRA, we want to be sure that the data is realistic. We know that cyber risks are always changing and always prevalent. We know that even with unlimited funding there is no such thing as a perfect cyber-protected system. And therefore, there is no value in pretending that all the systems are perfectly cyber-secure.

In the UK we have seen companies stop believing they are impregnable to cyber-attacks. Leaders and decision-makers have largely stopped denying the reality of cybersecurity threats and accept that there is only so much they can do. The stigma of falling victim to a cyber-attack has also substantially diminished, with reporting and sharing of incidents common (though it is still painful). This is a far more useful and mature cyber behaviour, as it allows whole communities to consider the best options, understand what measures were taken, and fight back. And this approach helps to ‘save face’, as many cyber incidents will become public knowledge very quickly anyway.

So, for the NCRA, please don’t let the CII organisations pretend their cyber defences are perfect, as we know they never will be. And no one expects them to be, for risk management means that you focus on the most important elements, with cost effective measures. Perfection leaves little political room for manoeuvre, or reasons to invest in cyber security improvements. And can result in unwelcome ‘career-limiting’ questions when a cyber-attack does eventually succeed against your system.

Although not ideal, these are some of the responses that we are likely to find:

* Poor board level awareness of the risk to the organisation
* Incomplete or missing corporate records including third party or inter-group contracts and policies
* Lapsed staff training on cyber security
* Cyber security policies repeatedly not followed
* Misunderstanding the cyber risks from supply chains / outsourced providers
* Deferred investment in security
* Poor data governance (particularly in test or product development environments)
* Staff work arounds compromising security systems because the agreed way of working is not the easiest way of working
* Misconfiguration of systems leaving them open to long-known vulnerabilities.
* Overconfidence in their understanding of their vulnerabilities (all low)