CRO Forum input to on DHS Cyber Incident data categories.

The CRO Forum appreciates the DHS effort to promote a robust cybersecurity insurance market, in order to improve public and private sector resilience to cyber risk, through the establishment of an effective, anonymized and trusted data repository.

Importance of a common codification

A common codification and taxonomy will help the reporting of cyber incidents and losses. It can facilitate greater understanding of cyber threats and improve society's cyber resilience. A common codification of standards and taxonomy can also support the underwriting and pricing of cyber risk.

The CRO Forum has been working on a categorization methodology for cyber risk. The objective is to enable cyber incident data to be collected using a common language and in a form that can ultimately be aggregated and shared in an anonymous form. The proposed methodology leverages existing reporting that occurs within IT and Risk Management functions, in order to encourage consistent data capture and reporting.

Issues to be addressed to ensure an effective data repository

The CRO Forum recognizes the significant challenges around an effective data repository, particularly how to ensure accurate, consistent and comparable reporting.

Where possible, data categories should limit the scope for subjectivity and, as a result, inconsistent reporting among entities. Inaccurate or inconsistent data would, of course, significantly reduce the value of the repository and the associated categorization methodology.

Another important challenge is ensuring anonymity. Anonymity of reporting is a critical element of an effective cyber incident data repository. Any cyber incident data repository needs to ensure anonymity while gaining the necessary level of detail to be effective.

The CRO Forum is in the process of finalizing a paper on a proposed cyber risk categorization methodology for discussion and to engage in the dialogue on this topic. The aim is to publish the paper in Q3 2016 and we are happy to exchange ideas with DHS before the publication. We look forward to a dialogue with DHS and other stakeholders on our shared objective of improving cyber resilience, including through the potential for effective cyber incident data sharing.

The CRO Forum appreciates the opportunity to comment on the DHS cyber risk data categories established in support of a cyber incident data repository.

CRO Forum
Website: *www.thecroforum.org*
E-mail: croforum.office@kpmg.nl