

PRESS RELEASE

For immediate release

Contact:

Caroline Dupuy

caroline.dupuy@lu.ey.com

Luxembourg, 7 April 2017 - 69% of businesses based in Luxembourg and surveyed as part of the FEDIL-ICT and EY joint study “*2016 Luxembourg Cyber security study*” just published today, recognize that a larger part of their investments should be assigned to cyber security. Businesses acknowledge the need to invest in this area more than they currently do, while also learning to make the most efficient use of it.

Cyber security has now become a critical board level issue, which can no longer remain the responsibility of the IT department alone. The C-suite has also definitively a role to play. Even more, business stakeholders need to understand and support initiatives that will help them defend their organization against cyberattacks, and also respond to potential breaches.

7 April was undoubtedly a red-letter day in the agendas of CEOs, CFOs and CIOs as it has just been the presentation of the second edition of the “Luxembourg Cyber security” study by FEDIL-ICT, in partnership with EY Luxembourg.

This study was carried out in collaboration with providers of essential services in the country, with the aim of defining a corpus of 50 hygiene rules for cyber security, based on shared experiences, new requirements from EU regulations, including GDPR, NIS Directive, and aligned with the objective 6 of “The National Cyber Security Strategy II” (*“Implement norms, standards, certificates, labels and frames of reference for requirements for the government and critical infrastructures”*).

As stated in the information note issued by FEDIL-ICT in March 2016, close collaboration of all key actors of the country has resulted in a clear, adaptive and practical security framework.

Through the 2016 Luxembourg Cyber security study, FEDIL-ICT in collaboration with EY Luxembourg has made it possible to introduce the first national corpus of hygiene rules for cyber security, which aims to support the Luxembourg Government and other national security agencies to keep momentum of cyber security in a more practical way and to position it as a matter of high priority, particularly to remain an attractive and competitive location for all companies already doing business or aiming at setting up their ICT operations in Luxembourg. But even more, this national corpus of hygiene rules is intended to support companies while bringing them with new rules to facilitate the creation of a strong cybersecurity ecosystem.

As part of this study, preliminary discussions were held with the Ministry of Economy and the Ministry of Media & Communications and are opening up promising future perspectives within the framework of the Digital Lëtzebuerg initiative.