


**RISK IN FOCUS 2021**

WEBINAR

**Cybersecurity:**  
What is the role of the human factor and how can internal audit challenge the existing practices?

**December 10th**  
from 1.00 pm to 2.00 PM  
(Central European Time zone)



**International round table organised by the European Institutes of Internal Auditors and the European Confederation of Institutes of Internal Auditing**

**Speakers:**

**Guy-Philippe Goldstein:** Advisor to PwC France, Researcher, Professor at Economic War School, the Autor of the expert's note in the Cyber Practical Guidance

**Luca Laguardia:** Head of Internal Audit Borsa Italiana , Member AIIA Cybersecurity Observatory

**Twan Oosterveld:** Group Internal Audit - IT audit & security at Citco

**Marc Solé:** Operational & IT Risk Audit Director at Banco Sabadell

**Facilitator:** Pascale Vandenbussche-ECIIA Secretary General

**Key messages:**

**Context:**

- Cybersecurity is a top risk that has increased with teleworking and digital infrastructure.
- The EU strives to ensure that "state of the arts" response is made to cybersecurity.
- The NIS Directive is currently assessed, and the report will be ready begin 2021 .
- In 52% of cyber incidents, human factor is the most important factor.
- The human factor is due to cognitive limitations or the absence of protocol respects or insider threat
- Everybody confirms the human factor is a key risk but one the most difficult one to assess!

## What are the good practices?

- "It is good to know who your enemies are"
- The cyber risk profile is changing all the time and Covid impact is a good example...so procedures must be continuously adapted, and you must react quickly
- Internal audit must help "by setting the tone", looking beyond the paper and see how people work
- Governance is important: *"If the Board of Directors is not in charge of cyber, it is hard to get everyone in the company combating cyber risks!"*, internal auditors must participate in all Committees (Management, Technology....) to stay connected with everyone
- Constant exchanges with the second line and with the peers are important to assess the risk
- Cyber exercises are important, but the scenarios must be complex, and the Management must be involved
- Internal auditors must test the different layers of the organisation and involve businesspeople in the tests. Organising a *"meaningful, real attack simulation"* is the best audit test!
- Evaluating the financial impact can help getting the involvement of the employees, the Board.
- Auditing the culture is not easy but help increasing the resilience.
- Training everyone about cyber risks is key and specialised training (eg about phishing) or the audit team is useful
- *"Cyber is about technology and human factor but we must not forget the importance of a strong governance system and a solid risk management!"*