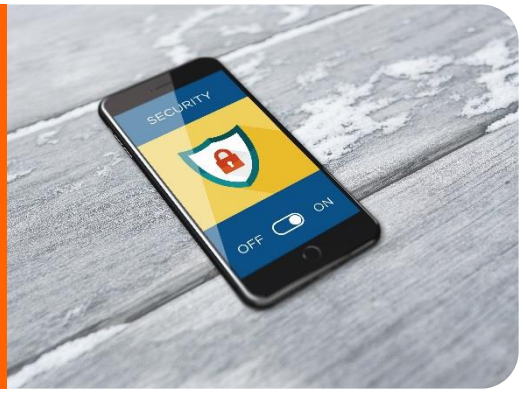
Cybersecurity

Strengthen private-public collaboration against cyber threats



"Our customers expect us to be a safe partner for their personal and business needs. We recognize this as a top priority, making cybersecurity a key part of ING's ambition to be a secure and trusted platform partner.

At ING, we raise customer awareness, train employees and invest in new technologies, such as AI, to keep up with the increased speed and quantity of new cyber attacks.

Cybercrime travels across sectors and across borders. This challenge thus needs a common response. Both companies and public authorities should work on combating cybercrime together. The EU plays an important role in endorsing this collaboration and providing an effective regulatory framework."

Roel Louwhoff
Chief Operations Officer ING Group

Cybercrime forms a growing threat to companies in general and to the financial system specifically. Cyber attacks are becoming more frequent, and more intense. At the same time, banks become more exposed, as they digitalize, rely more on cloud computing, and are increasingly connected to 3rd party providers. Cybersecurity can be seen as a 'rat race' between cyber criminals' attacks and their targets' response. Accordingly, costs for cybersecurity are increasing, as are potential losses in case of a successful cyber attack.

We encourage financial & other sectors, law enforcement authorities, governments and internet service providers to collaborate in combating cybercrime. Given the scale and cross-border nature of cyber threats, the EU plays an important role in strengthening cybersecurity. We therefore recommend to pursue the following initiatives:

- Set up a European platform for cybersecurity intelligence and information exchange, to strengthen operational collaboration between both private and public players across borders;
- Harmonise the EU regulatory and supervisory framework for cybersecurity and make it more risk-based by focusing on actual cyber threats.

Finally, it is important to ensure a coherent approach to cybersecurity. Data privacy and cybersecurity can co-exist to the benefit of all those concerned.

Today's legislative framework for cybersecurity

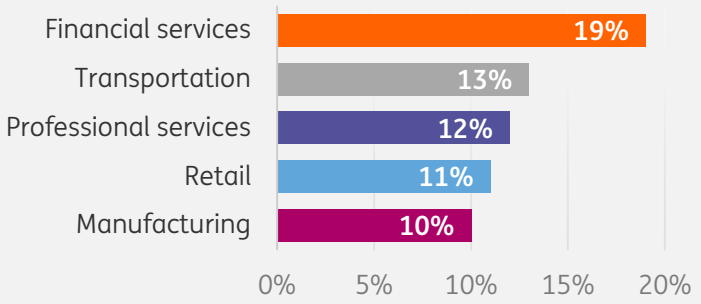
The European Commission has identified cybersecurity as one of the main challenges in its 2017 mid-term review of the Digital Single Market. The Network and Information Security ("NIS") Directive (2016) is considered to be the first piece of EU-wide legislation on cybersecurity. It requires essential service providers to take appropriate security measures and report serious incidents. Additionally, the revised Payment Services Directive ("PSD2") introduced enhanced security & authentication requirements for electronic payments, while the General Data Protection Regulation ("GDPR") requires institutions to protect the personal data of their customers. Banks also need to hold capital against cyber risks as part of the Capital Requirements Regulation's ("CRR") operational risk framework.

The recently adopted EU Cybersecurity Act gives ENISA, the EU Cybersecurity Agency, a reinforced role and establishes an EU-wide cybersecurity certification framework for digital products, processes and services. This is complemented by the European Supervisory Authorities' ("ESA") advice to improve ICT risk management requirements, streamline incident reporting standards and establish an EU-wide cyber resilience testing framework.

Despite these initiatives, the legislative landscape remains fragmented with Member States to a large extent responsible for cybersecurity issues. In addition, different interpretations by national authorities of EU rules (e.g. GDPR) lead to uncertainty and prevent a quick and collaborative response to cyber attacks.

ING

Most frequently targeted industries in 2018*
% of total cyber attacks



Source: IBM X-force

Alongside a growing number of security breaches, the total cost of cyber attacks for the average company increased from US$11.7 million in 2017 to a new high of US$13.0 million – a rise of 12% (Source: Accenture).

*based on responses from 355 companies (Australia, Brazil, Canada, France, Germany, Italy, Japan, Singapore, Spain, the United Kingdom and United States)

Information exchange and collaboration

To address the increased threats stemming from cybercrime, it is important to set up a European platform to share cyber intelligence and incident information between private sector firms and competent authorities. Voluntary information sharing will help institutions identify cyber attack trends and co-develop best practices on cyber resilience with the aim to prevent, withstand and recover swiftly from disruptions.

Information sharing requires trust between members. Most European banks have already agreed not to compete on cybersecurity. This can be further enhanced by endorsing information exchange at EU level. Additionally, a common cyber taxonomy that allows for operational information exchanges is necessary. The Financial Stability Board's Cyber Lexicon is a good starting point to further develop a set of core terms related to cybersecurity in the EU financial sector.

Finally, barriers to information exchange should be removed. Privacy concerns arise concerning disclosure of personal information due to a lack of explicit exemptions in the GDPR and differing interpretations by national data protection authorities. The European Data Protection Board should clarify how information sharing and processing of personal data is allowed under the GDPR. Personal data will be more secure when institutions can share mostly anonymous information, when necessary and proportionate for the purpose of cybersecurity.

Harmonise and improve EU regulation

A number of Member States implement their own regulatory frameworks for cybersecurity. Despite convergence in high level expectations, the technical specifications and supervisory practices differ across jurisdictions, leading to a complex and fragmented regulatory landscape across Europe. As noted in the recent ESAs' advice, it is important to harmonise cybersecurity requirements, where possible.

Additionally, ING is in favour of cybersecurity being addressed more on the basis of actual cyber threats, and less by rule-based compliance. Regulation will be most effective when it is proportionate to an institution's size, internal organisation, and the riskiness of the products and services. The ECB's TIBER-EU framework for cyber resilience testing is a good example.

ECB TIBER EU Framework
Threat Intelligence-based
Ethical Red Teaming

EUROPEAN CENTRAL BANK
EUROSYSTEM

- TIBER EU is the 1st European framework for controlled cyber hacking (2018)
- A Red Team performs 'Ethical hacking' to test the cyber resilience of financial market entities
- Critical systems are tested on actual, real-life threats
- Testing helps entities gain insight about their protection, detection and response capabilities

We thus support the recent ESAs' advice to establish a coherent cyber resilience testing framework across the EU financial sector. Consistent application of this framework should allow for mutual acceptance of the test results by competent authorities. The European Commission, with the support of the ESAs, ENISA, ECB and national competent authorities, can facilitate the establishment of such a framework in collaboration with private sector representatives.

Furthermore, institutions currently perform several types of incident reporting related to cybersecurity. Streamlining the incident reporting procedure through the standardisation of the reported breach information will facilitate knowledge exchange across the EU. It will help affected institutions to address cyber attacks in a timely manner by avoiding a duplication of efforts. Finally, incident reporting will be most effective if combined with a reciprocal system of timely, risk-based information sharing between public authorities and the private sector.

To protect the financial system from a growing systemic risk, combating cybercrime should be seen as a common challenge for companies and public authorities. The EU is well placed to contribute to cybersecurity by endorsing information exchange and collaboration, and by providing a harmonised, mostly risk-based regulatory framework.

Regulatory & International Affairs
+31 20 576 6388

ING