Cybercrime: NIS Directive & GDPR what's new and what to do ?

(Spring conference EYBA – 7 April 2018)

A new European framework of cybersecurity

Bertrand WARUSFEL

Partner (FWPA Law firm)

Professor at Paris 8 University

bwarusfel@fwpa-avocats.com

Why the European Union is bulding a cybersecurity framework ?

- UE supports the development of an european Information Society
- Security and defense topics became major subjects of the European policy (fight against terrorism, police cooperation, area of freedom, security and justice, ..)
- Non harmonized security practices could be an obstacle to the circulation of data
- Data security is one of the requirements of the new GRPR

bwarusfel@fwpa-avocats.com

Recent UE regulations related to cybersecurity

- Regulation n° 526/2013 concerning the European Union Agency for Network and Information Security (ENISA)
- Directive n° 2013/40 of 12 August 2013 on attacks against information systems
- Regulation n°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)
- Directive n° 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)

+ GDPR provisions related to data security (art. 32-34)

Regulation n° 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA)

- Definition of 'network and information security' : « the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems » (art. 1.3)

- (ENISA) « shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union » (art. 2.3)

Directive n° 2013/40 of 12 August 2013 on attacks against information systems

- « This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems » :
  - illegal access (art. 3)
  - Illegal system interference (art. 4)
  - Illegal data interference (art. 5)
  - Illegal interception (art. 6)
  - tools used for committing offences (art. 7)

  (offenses already defined in the Council of Europe *Cybercrime Convention* - Budapest, 11/2011)

Regulation n°910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market

(eIDAS = **E**lectronic **ID**entification **A**uthentication and trust **S**ervices)

This Regulation:

- (a) lays down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;

- (b) lays down rules for trust services, in particular for electronic transactions; and

- (c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication (art. 1)

bwarusfel@fwpa-avocats.com

eIDAS : a public/private cooperation for digital security

- On the public side :
  - Mutual recognition of electronic identification means used by public digital services
  - Use of trusted services by public bodies (electronic signature, seals …)
- On the private side
  - use of the same trusted services by private entities
  - but control and supervision by each national security authority

eIDAS trust services

- electronic signatures (art. 25)
- electronic seals (art. 35)
- certificates for website authentication (art. 45)
- electronic registered delivery service (art. 43)
- preservation services (for signature or seals)

based on qualified certificates delivered by trusted service providers

qualified and controlled, under the supervision of a national digital security authority

bwarusfel@fwpa-avocats.com

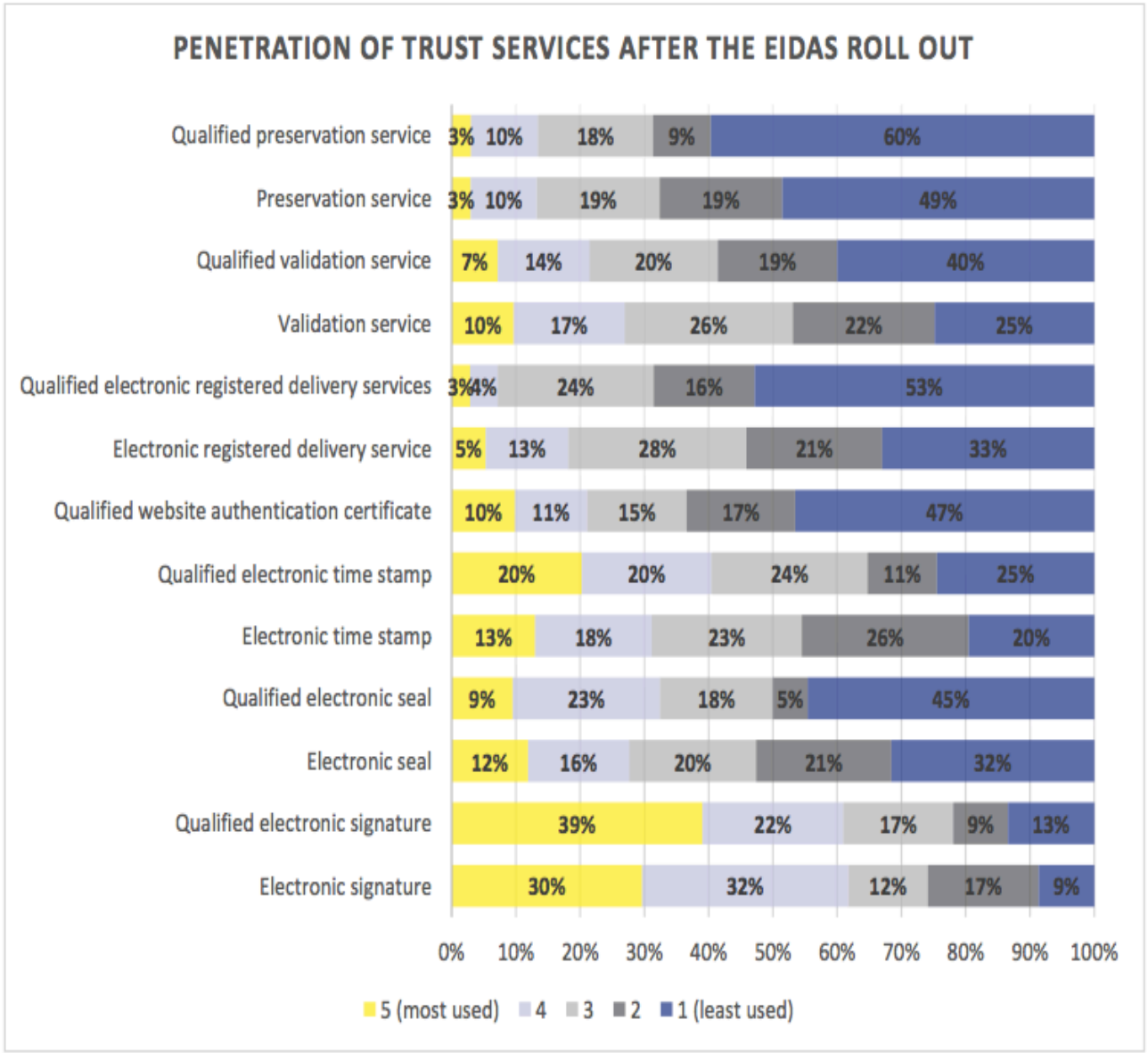


Figure 5 Trust services penetration in the market one year after the eIDAS roll-out

bwarusfel@fwpa-avocats.com

Directive n° 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)

- « Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems » (art. 3)
- The criteria for the identification of the operators of essential services :

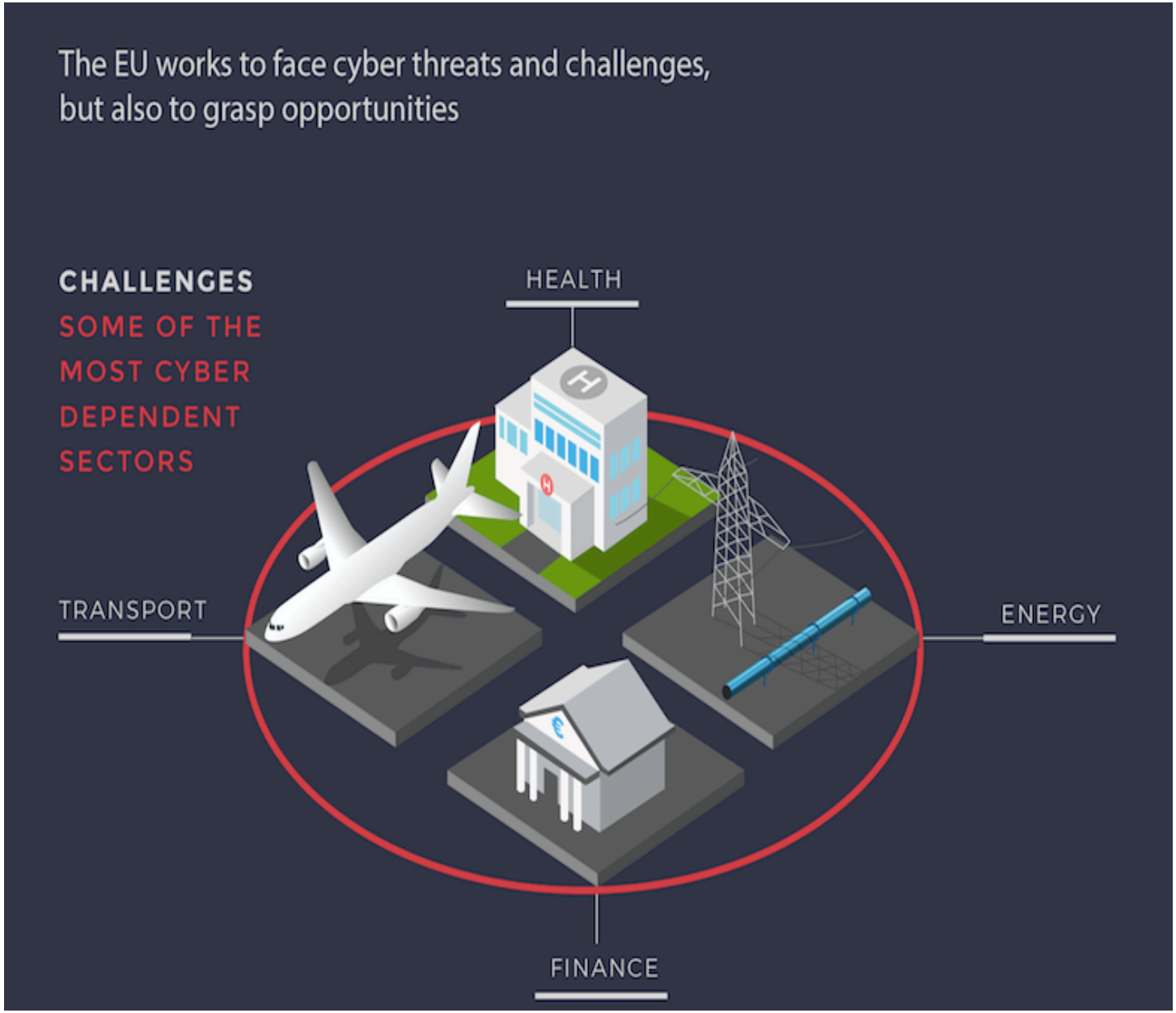
  (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

  (b) the provision of that service depends on network and information systems; and

  (c) an incident would have significant disruptive effects on the provision of that service (art. 5.2).
- Member States
  - « shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations » (art. 14)
  - « shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems » (art. 16)

  + Obligation to notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the services they provide
- Organisation in each Member State : 1 national competent authority
  + 1 Computer security incident response team (CSIRT)

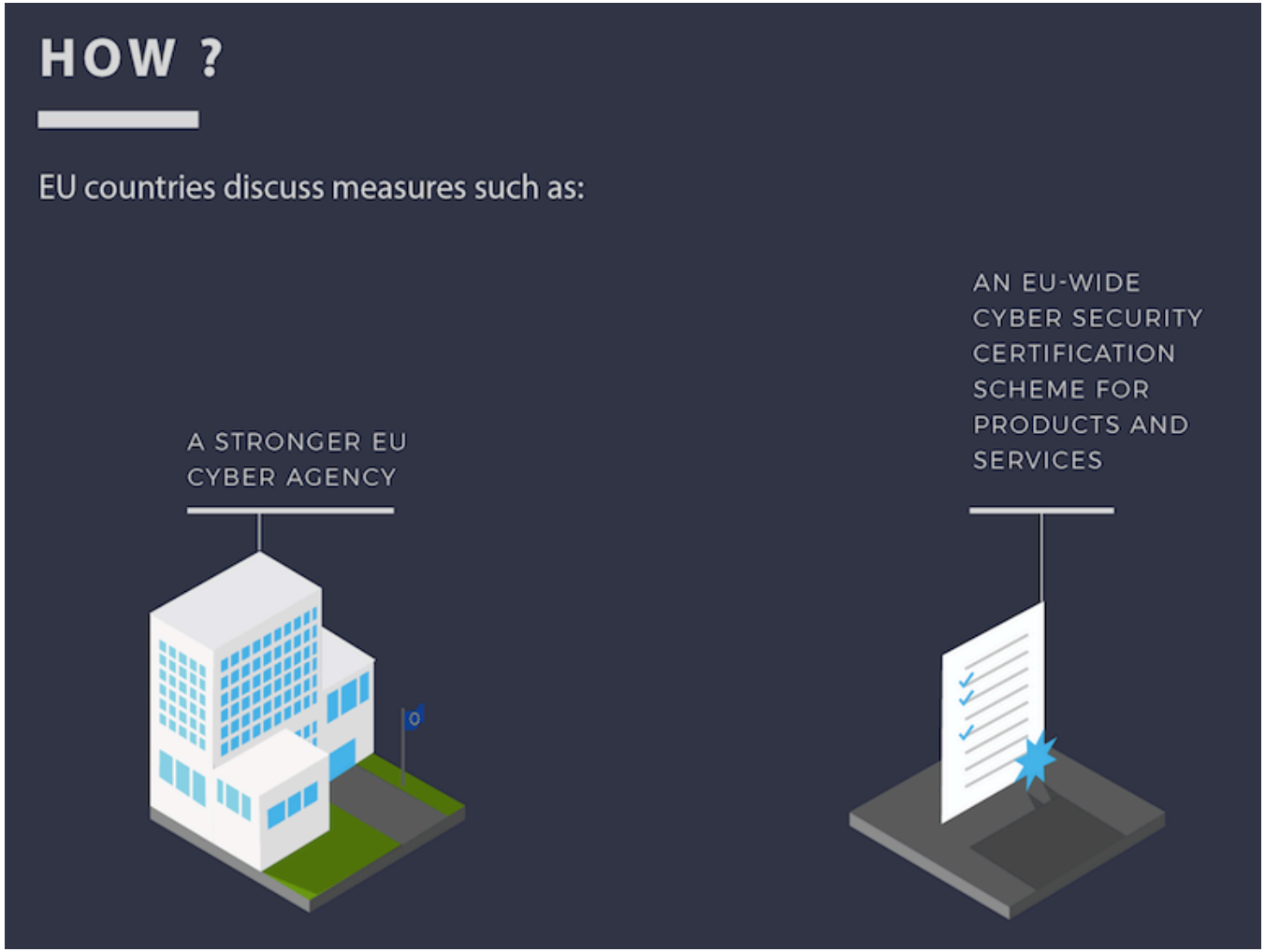
bwarusfel@lwpa-avocats.com



bwarusfel@fwpa-avocats.com

Next steps proposed by of the UE Commission (october 2017) :

- A new regulation regarding ENISA
- A Cybersecurity Act (European Cybersecurity certification Scheme)



bwarusfel@fwpa-avocats.com