Deloitte.

# “State of the Art” in Cyber Security

Luigi Bruno, LL.M. | 20 June 2019

# "State of the Art" and the Law: An Unclear Relationship

Regulators are requiring organisations to implement state of the art security measures: what does it concretely mean for organisations? GDPR and the NIS Directive as an example.

**GDPR**

**Article 32**

**Security of Processing**

*"Taking into account **the state of the art**, the costs of implementation and the nature, scope, context and purposes of processing […] the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate."*

**NIS**

**Article 14**

**Security Requirements and Incident Notification**

*"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. Having regard to **the state of the art**, those measures shall ensure a level of security of network and information systems appropriate to the risk posed."*

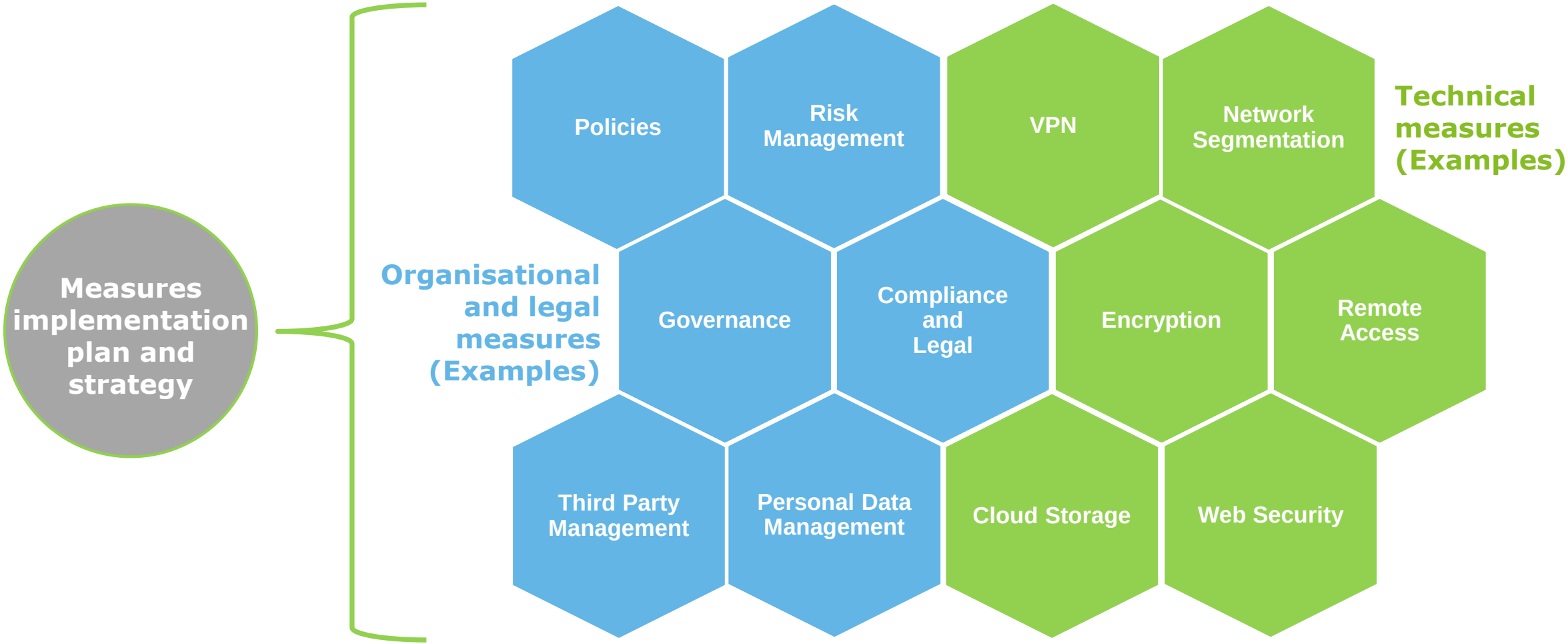
The General Data Protection Regulation (EU) 2016/679 (**GDPR**) and the Directive on the Security of Networks and Information Systems (EU) 2016/1148 (**NIS Directive**) require organisations in order to be compliant to implement security measures that take into consideration **the "State of the Art": i.e. chosen based on a consensus of professional opinions**[1].



1. Source: IAPP 2019

# “State of the Art” and Organisations: A Clear(er) Relationship

Implementing state of the art measures requires a coordinated effort across the organisation – both from a technical and organisational perspective.



# Implementing Effective "State of the Art": A Coordinated Journey

Many organisations fail to leverage their measures implementation efforts due to a lack of communication and coordination between key internal stakeholders.

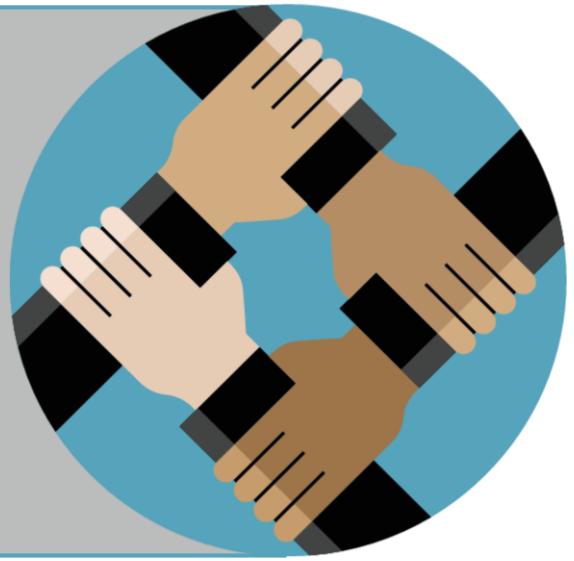
Our experience has shown that a number of organisations **do not effectively prepare key departments to coordinate to leverage compliance and security measures to prevent, resolve, and report cyber security and data incidents** in line with current **cyber** and **data protection regulations and laws.**

As a consequence, many incidents **are not resolved and reported in time, thus posing severe stress upon DPOs, Legal Counsels, CISO and other C-level stakeholders**, as well as **exposing the business to fines and consumers to risks.**

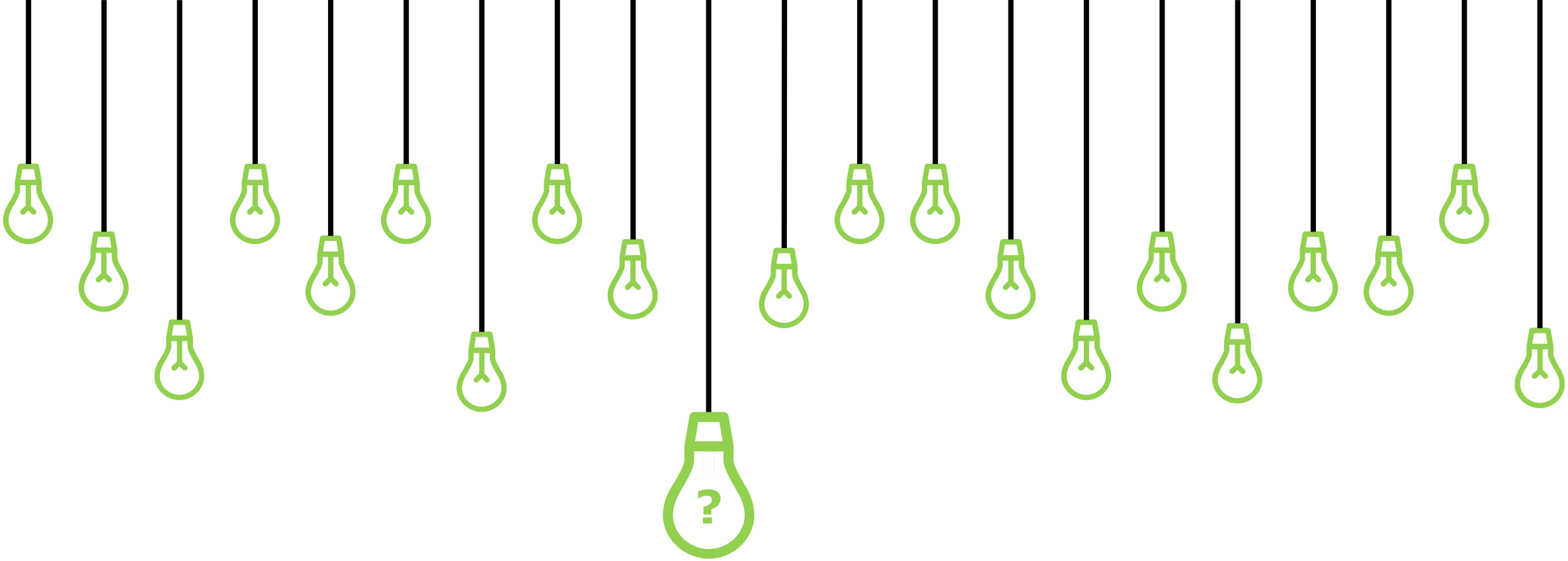
# Hoping for the Best, Prepared for the Worst

Simulating and reading cyber security incidents: preparing stakeholders and departments to leverage implemented measures to jointly resolve and report incidents in a compliant way.

Incident simulation is fundamental to achieve closely-knit **cooperation** between **all relevant stakeholders** to **resolve and report incidents in an effective and compliant way**. Therefore, **DPOs, CISOs**, **Legal Counsels**, **Compliance Officers,** and **C-Suite stakeholders**, must be **prepared to communicate and swiftly coordinate following incidents** to **jointly execute on the best course of action**.



- **Knowing what to do in a cross-functional collaborative manner is the true "State of the Art"!**
- **Security challenges cannot be confronted in silos!**




# Thank you for your attention!

**I am more than happy to answer your questions.**

Deloitte.