EXECUTIVE ADVISORY REPORT

European Union Cybersecurity-Related Legislation

Resolving the "State of the Art" Paradox

The new Network and Information Security (NIS) Directive and General Data Protection Regulation (GDPR) combined will require all organizations that are in, or do business with, the European Union, to incorporate 'state of the art' into their cybersecurity.

OVERVIEW

By the end of May 2018, the GDPR and NIS Directive will have entered into force in the European Union, giving organisations covered by these pieces of legislation until this date to establish compliance. Both pieces of legislation require companies to 'take into account' and 'have regard to' state of the art (in GDPR and NIS, respectively) for their cybersecurity. However, neither piece of legislation defines the term or mandates use of specific technologies. This was a conscious decision, as security capabilities and IT evolve quickly, while legislation is typically long-term. The EU, therefore, places the onus on industry to maintain an understanding of what the current security capabilities and best practices are in the market.

STATE OF THE ART PARADOX

Companies must therefore have a view on what 'state of the art' means to them and be prepared to defend that view. This point is critical: in any post-breach investigation (NIS has notification requirements around security incidents, whereas GDPR on personal data breaches) a company will likely have to defend its use — or lack of use — of a range of technologies.

IDC and Palo Alto Networks recently joined together to gauge how prepared potentially covered organisations believe they are to meet these new requirements as well as their understanding of what constitutes state of the art. The results yield a 'state of the art paradox': while most organisations believe that they are already compliant with the new rules, the vast majority have a poor understanding of the concept of state of the art, have no processes or metrics in place to measure alignment with the concept, and do not review their position on it with sufficient frequency.

Who does the NIS Directive apply to?

The NIS Directive applies to **operators of essential services** and **digital service providers**.

- Operators of essential services include companies providing transportation, energy and healthcare services. Member states are responsible for identifying the companies in these categories.
- Digital service providers are companies that provide one of three services: cloud computing services, online marketplaces, or online search engines.

Who does the GDPR apply to?

The GDPR applies to companies that meet any of the following criteria:

- Are established in the EU.
- Offer goods or services to EU residents.
- Monitor the behavior of EU residents that takes place within the European Union.

BUILDING A READINESS PLAN

In order to address this knowledge gap, CEOs need to ask some fundamental questions about their companies' readiness for GDPR and/or the NIS Directive. Ask your CISO and Chief Privacy Officer:

A. Does GDPR or the NIS Directive, or both, apply to our company? Who in the business is accountable for these legislative requirements?

B. What is the company view on state-of-the-art security? How did we define it, and who advised us on this?

C. What is the timescale for us to reach compliance, and what actions need to be taken now in order to achieve compliance by the deadlines?

D. How will the business continue to maintain compliance, and what metrics will the business use to validate this to itself and, when required, to any third parties?

TAKE ACTION

Download the **full report** from IDC. Speak to your Chief Privacy Officer, CISO and CIO about keeping pace with the leading capabilities to protect the personal data of EU residents as well as sensitive business data. Speak to your legal department to determine whether you are covered by either the NIS Directive or GDPR or both. Determine your preparedness to comply with the laws and to monitor the laws' implementation in the EU countries in which you do business.