KCS Group Europe

The cyber threat: a matter of compliance

01/03/2018

2018 is the year of cyber. In spring two important pieces of EU legislation will come into force: the Network Information System (NIS) Directive and the General Data Protection Regulation (GDPR). Failure to comply with the requirements will impose heavy fines on businesses. Therefore, the government is stepping up against the cyber threat in legal terms, but recent events, such as the WannaCry attack, proved that the government itself is not prepared yet.

The NIS was adopted by the European Parliament in 2016. Member States then had 21 months, until May 2018, to transpose what was highlighted in the directive into their own national law. The aim of the legislation is to strengthen cyber security capabilities, along with increased cooperation within State Members. The NIS also introduced new incident reporting obligations. Non-compliance will result in heavy fines of up to £17 million being imposed on businesses, and all expectations are that early transgressions will be punished heavily – to deter any other would-be avoiders.

The NIS is concerned more about increasing preparedness for a cyber threat, while the GDPR focuses more on personal data security. However, the two almost overlap in regard to the incidents reporting requirements. In fact, the GDPR requires data breaches to be reported, within 72 hours of discovery, to the competent authority. Similarly as the NIS, non-compliance involves fines; which are two tiered and could be either €10 million or €20 million. The GDPR rules will be enforceable from 25 May 2018.

Businesses still have a few months to get ready to comply with the requirements and avoid possible fines. However, businesses are not the only ones who should prepare. The government and its infrastructures, as promoter of the new legislation, should already be prepared to face the cyber threat. Unfortunately this is not the case.

In a time where there is widespread concern about cyber-attacks and the government imposes strict requirements on business in order to boost their protection and preparedness, it appears that the government itself is not complying with its own demands. In fact, last year, the NHS was a victim of a ransomware attack, WannaCry due to inadequate security and defences.

KCS Group Europe

The cyber threat: a matter of compliance

In May 2017, 81 health trusts were affected by WannaCry, out of the 236 trusts in England, as well as other 600 GP surgeries, leaving sensitive data exposed. The worm spread from machine to machine and was later stopped by activating a killer switch that prevented more computers from getting infected.

Therefore, the government and its infrastructure should be better prepared for events such as WannaCry. They should be the first ones to implement their security measures as an example for other businesses. If the government cannot protect itself, why should it dictate to businesses how to prepare for a cyber threat, and how can it be seen as a credible gatekeeper of the cyber-security of the nation?

The National Cyber Security Centre (NCSC) has recently confirmed the possibility of a major cyber-attack targeting the UK; it just remains a matter of when that will take place. The government strategy turns to fines in order to deter people and increase compliance, but it is forgetting about its own infrastructures. Leadership by example would not go amiss.