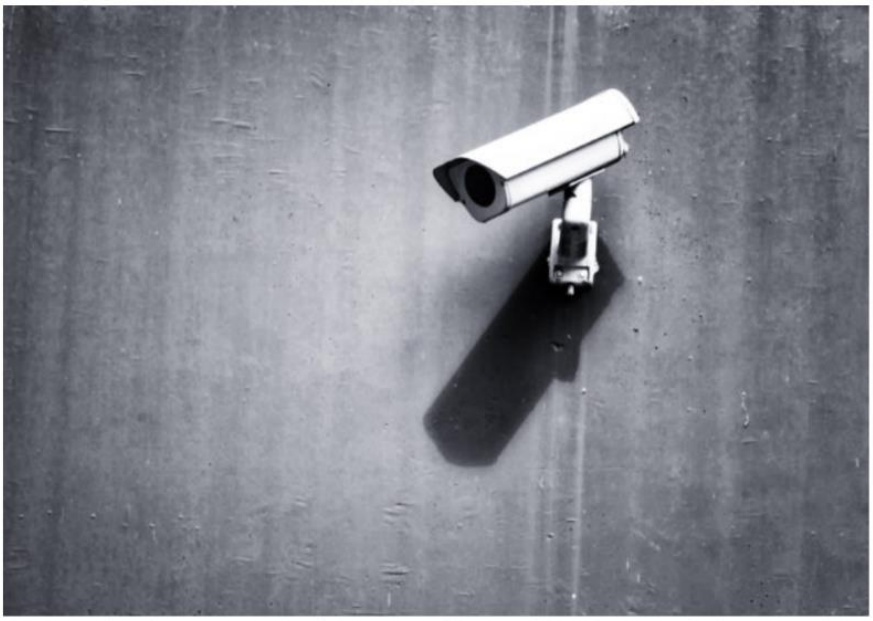
The GDPR is not all doom and gloom

Feature 19 SEPTEMBER 2017

Despite the complexities of the GDPR — it is time to start taking positive lessons from difficult situations



Ultimately, it will be whatever the CISO makes of it, however it would be remiss of them to be unaware of the huge amount of value they are able to add to their role, and their organisation, in the way they tackle this new legislation

Nick Ismail

In just over 6 months the oft dreaded General Data Protection Regulation (GDPR) will come into force, affecting businesses across the country. A lot of time has been spent and ink spilled laying out the hassle and negatives this regulation will bring.

Questions such as, "What do I need to be worried about?" and "How damaging will this be to my business?" are often heard in relation to the new European-wide legislation. You would be forgiven for thinking it's all doom and gloom come May 2018. For CISOs however, this is not necessarily the case.

Rather than viewing this as simply a challenge, or another hurdle to overcome, for CISOs it is an opportunity to demonstrate their value to the wider organisation, acting as a vehicle for positive change, and it's starting off in the right direction. ClubCISO's latest Information Security Maturity Report 2017 revealed that 79% of CISOs have actually received the extra funding they desperately need.

>See also: **Practical steps to deal with the GDPR**

FIND OUT MORE

And, with changes such as the GDPR coming, this couldn't have happened at a better time — hopefully giving these senior IT decision makers some leeway in implementing the right infosec tools and policies to make their organisations GDPR compliant.

However, the opportunity for CISOs goes far beyond a bit of extra cash. The role of the CISO is still relatively young in the corporate world, and thus is often found jockeying for its position among the ranks.

The GDPR may serve as a defining moment for the CISO. This is an opportunity to both add value to the organisation through vital knowledge of the security landscape, as well as cementing the role of the CISO higher up the C-Suite ladder.

Bossing the boardroom

In conference rooms up and down the country, there is often a disconnect between the board and the CISO when it comes to the management and deployment of infosec strategies. The root cause of this is in fundamental misunderstandings of the state of play when it comes to cybersecurity.

For example, the actual role of the CISO is largely considered, by the CISO at least, to be a strategic one. Despite this, however, many aren't involved with overall business strategy as part of their day-to-day job. While 37% of boards are claiming that this should be a greater area of responsibility for CISOs, it isn't currently an area they have great influence in.

To change this, the GDPR must take the front seat. It is imperative that CISOs take advantage of the recent willingness of boards to invest monetarily into information security, given the extensive effect it will have on the business. As well as this, it is key they embrace the influence they are now able to exert on other aspects of the company.

>See also: **6 steps to GDPR compliance**

For example, with the GDPR in particular, CISOs will be far more involved with the legal team and supply chain agreements. This is important, as these are always areas of high vulnerability when cyber criminals strike. Already, CISOs are taking this opportunity to work closely with vendors, controlling operations with third parties and tightening contracts from an infosec standpoint.

Operating, at present, from a role of relative isolation, the GDPR also gives the CISO the opportunity to form and bolster strong working relationships across their business, which, ultimately, can only be beneficial to the wider organisation. Through doing this, there is also an opportunity to foster good cybersecurity practices across a multitude of different departments and roles.

Shifting the security landscape

Prevention has always been the largest aspect of a company's approach to cyber security. However, focusing squarely on 'keeping out the bad guys' is no longer enough in the modern day organisation.

With a constantly shifting threat landscape, alongside unavoidable weak links in staff unwittingly (or wittingly) opening digital backdoors throughout large organisations, a breach is inevitable at some stage. If a company has spent its entire cybersecurity resource on prevention, its ability to mitigate, and recover from, the damage of an attack will certainly falter.

>See also: **One year to GDPR: guide to compliance**

CISOs too can capitalise upon this shifting landscape, educating the board that the game has changed, and explaining the need to foster holistic infosec practices which stretch far beyond the borders of the IT department. Fighting the core misunderstandings CISOs struggle against on a day-to-day basis should absolutely be capitalised upon.

The serious nature of ensuring GDPR compliance should not be ignored, despite the huge opportunity it presents. Ultimately, it will be whatever the CISO makes of it, however it would be remiss of them to be unaware of the huge amount of value they are able to add to their role, and their organisation, in the way they tackle this new legislation.

Sourced by Mark Lueck, Chairman, ***ClubCISO***