CISO + GDPR = A Force For Change

BY MARC LUECK ON 29/09/2017 · 106 VIEWS ANALYSIS, SECURITY

If you mention the GDPR (General Data Protection Regulation) amongst certain boardroom circles, the common reaction is for people to bury their heads in the sand and hide under tables. After all, the GDPR is just a fine waiting to happen, right? If the Information Commissioner's Office (ICO) deems your organisation culpable for a sensitive data breach, and finds you haven't done enough to safeguard that data — they'll be asking for the princely sum of €20 million euros or 4% of global turnover, whichever is greater.

It is understandable therefore that a regulation which has such extensive financial consequences for noncompliance evokes this sort of reaction. However, from the perspective of the Chief Information Security Officer (CISO), who is likely to be tasked with keeping the organisation safe from the 'dreaded GDPR', the regulation shouldn't create feelings of fear, but instead of determination and opportunity — and be thought of as a positive force for change.

In ClubCISO's recent Information Security Maturity Report 2017, 66% of those surveyed had seen an increase in their budgets this year, and the common consensus was that the GDPR has played a major part. And let's face it — additional finance for IT is always welcome, especially when security professionals are facing a threat landscape which is constantly growing in complexity.

But, aside from the monetary benefits, the GDPR should first and foremost be viewed as a vehicle for change. It is one of those critical moments in time that can help future cyber security leaders take charge and add value to their organisations.

Bolster That Relationship With The Boardroom

One of the major issues for the CISO today is the often clear disconnect between the role itself, and the board — about how information security can and should be managed. As evidenced by the Information Security Maturity Report 2017, many CISOs like to think of their roles as strategic, however as part of their day-to-day job, they rate strategy as a very low responsibility (just 6%). Their boards on the other hand think that CISOs should prioritise strategy more highly (37%), and in reality that broadly equates with the CISO's real life remit (35%).

The GDPR can help to balance these expectations — the very nature of the legislation means it certainly cannot be enacted by one person alone, and to achieve proper compliance, departments and working groups will have to come together. The CISO can act as the lynchpin in this scenario, utilising their expertise to forming working relationships with colleagues, and help to change the status-quo of IT — away from slow moving cost centre, and towards strategic problem solving machine. It also provides a chance for the CISO and IT to reinforce the importance of good cyber security practices across the organisation, with the backing of business leaders.

Don't Focus Solely On Prevention

Gone are the days where having a good antivirus client and firewall would safeguard sensitive corporate information — yet 78% of company boards still place their focus squarely on data loss prevention (DLP) capabilities, rather than response (just 22%). Preventing a breach is, of course, still incredibly important within the context of GDPR compliance. However, contrary to popular belief, companies will not get an automatic fine should a breach occur.

Popular


Top 10 Benefits Of Tablet PCs


8 Facts Why SEO Is Critical For Your Digital Marketing Strategy

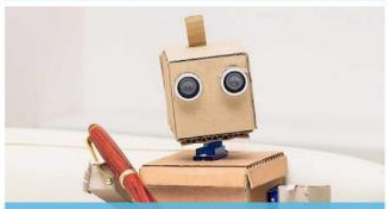

Reimagining IT In A World Of APIs


5 Reasons Why Video Advertising Is Necessary In Today's Digital World


Top 5 Upcoming E-Commerce Mobile App Trends

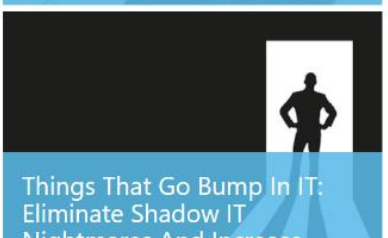
Latest


Accurate Testing Will Guide Us To The 5G Future


How Artificial Intelligence Can Make The Difference For Customer Service


Harnessing The Full Potential Of A Connected Customer


Citizen Developers And Low Code Application Development


Things That Go Bump In IT: Eliminate Shadow IT Nightmares And Increase Governance And Security Compliance

Instead, as long as an organisation has been deemed to do enough to safeguard sensitive intellectual property, then it will be protected against penalisation from the ICO. Again, the GDPR offers an opportunity for positive change, encouraging CISOs to focus on prevention and recovery — in equal measure — and this reality gives them legitimate reason to engage the board in a conversation about the importance of a balanced infosec strategy.

The GDPR is certainly complex, and should not be downplayed. But it is also full of opportunity. It just needs CISOs to take stock, and focus on the positives. After all, it was George Bernard Shaw that once said, "progress is impossible without change, and those that cannot change their minds cannot change anything" — and it's never been more true. View the GDPR as a force for positive security change, then that's exactly what will happen.

Marc Lueck

Marc Lueck is a senior security practitioner with over 20 years of experience crossing multiple industry sectors, from financial services to publishing. For the past 7 years, he has led security improvement programmes for the likes of Pearson, T-Systems and Symantec. He is currently the CISO at Company85, where he runs the security practice with a focus on ensuring information security enables and supports business goals.