ForeScout

Impact of GDPR on IT Security Spending

October 6, 2016

By Dan Lamorena (https://www.forescout.com/company/blog/author/dan-lamorena/)

Vice President, Global Field Marketing & Lead Development

Last week I had the pleasure of attending the UK CISO Summit (http://www.cisosummit.co.uk) held in London. The event, attended by 40 of the UK's top security folks, is designed to encourage information and best practice sharing amongst peers. Topics included planning for IT () security spending, optimizing your Security Operations Center (SOC), best practices for training your employees on security, and how innovations in quantum computing will affect security (i.e. cause nightmares by breaking current encryption techniques).

The hottest topic at the event was what the General Data Protection Regulation (GDPR ()) is and how it will impact UK firms. The intent of the GDPR () is to give citizens of the EU control over their personal data and unify data privacy and protection regulations across the EU. Fines for noncompliance could be a maximum of

20M Euros or 4% of global turnover depending upon which is larger.

I led a discussion on the annual fight for IT () security spending and some of the techniques that are being used to get more funding. Gartner predicts the global IT () security spend

(http://www.gartner.com/newsroom/id/3404817) in 2016 will be approximately $82B and many analysts are predicting growth (http://cybersecurityventures.com/cybersecurity-market-report/) between 8-12% over the next 5 years.

When I polled the audience, though, nearly all attendees did not see an increase in their IT () security spend in 2016. As noted by a CISO, IT () projects that have a notable ROI () that drives top-line business are often prioritized over security projects.

Compliance and new regulatory standards are often a great impetus for sought after budget increases. GDPR () will require companies to look at new ways to store and protect data, ensure continuous monitoring of IT () assets, and hire new personnel. The regulations are active on May, 2018 after a two year transition period that began earlier this year. However only one hand was raised in the audience when I asked if GDPR () would increase their IT () security spending in FY17. Interestingly, most firms appear to be taking a "wait and see" approach on how GDPR () will be monitored and regulations enforced. Interestingly, most felt BREXIT wouldn't have much of an impact on compliance, because most firms conduct business in the EU countries and would be subject to GDPR () regardless.

In terms of what is successful in obtaining additional budget dollars, one notable CISO joked that his charming personality was the main reason he was able to get more budget than his IT () peers. For those less charismatic CISOs, they have increasingly been doing risk assessments and creating frameworks to communicate to their Boards the risk that the company is exposed to, how that risk can be mitigated through increased security controls, and the necessary increase in IT () security spending required to mitigate those risks. That being said, Boards are composed of outstanding business people who calculate risk and make important decisions on a regular basis. The answer isn't always to eliminate risk – all the budget in the world will not accomplish this – but to determine what risk is acceptable for the organization. As "Mr. Congeniality CISO" above would later mention, business executives live with way more risk in the course of their regular business activities than the probabilities of a particular security control not being enacted and a breach occurring. Perhaps this best explains the current approach for most organizations on GDPR (). Until, there is a better sense of the penalties attached to GDPR () and the risk of being out of compliance, the cost to maintain that compliance isn't proving to be worthy of investment.

Dan

Products (https://www.forescout.com/products/)

CounterACT® (https://www.forescout.com/products/counteract/)

Extended Modules (https://www.forescout.com/products/extended-modules/)

Enterprise Manager (https://www.forescout.com/products/enterprise-manager/)

Solutions (https://www.forescout.com/solutions/)

Internet of Things (IoT) (https://www.forescout.com/solutions/iot/)

Campus (https://www.forescout.com/solutions/campus-cybersecurity/)

Data Center and Cloud (https://www.forescout.com/solutions/data-center/)

Operational Technology (https://www.forescout.com/solutions/operational-technology/)

Industries (https://www.forescout.com/solutions/industries/)

Use Cases (https://www.forescout.com/solutions/use-cases/)

Partners (https://www.forescout.com/partners/)

Technology Partners (https://www.forescout.com/partners/technology-partner-program/)

Reseller Partners (https://www.forescout.com/partners/resellers/)

Partner Portal (https://forescout.channeltivity.com/)

Company (https://www.forescout.com/company/)

About Us (https://www.forescout.com/company/about-us/)

Board of Directors (https://www.forescout.com/company/board-of-directors/)

Investor Relations (https://investors.forescout.com/)

Careers (https://www.forescout.com/company/careers/)

News (https://www.forescout.com/company/news/)

Resources (https://www.forescout.com/company/resources/)

Press Kit (https://www.forescout.com/company/press-kit/)

Blog (https://www.forescout.com/company/blog/)

Legal (https://www.forescout.com/company/legal/)

Support (https://www.forescout.com/support/)

Get Support (https://www.forescout.com/support/get-support/)

Support Programs (https://www.forescout.com/support/support-p

Customer Service (https://www.forescout.com/support/services

Training (https://www.forescout.com/support/training/)

REQUEST DEMO (/DEMO/)

Contact Us (/contact-us/)

Toll-Free (US):   1-866-377-8771

Tel (Int'l):   +1-408-213-3191

Customer Login (https://www.forescout.com/support/login/)

Find a Reseller (https://www.forescout.com/partners/resellers/)