Trend Micro Study Finds ‘State of the Art’ GDPR Rule Confuses Businesses

Businesses more concerned with security costs than meeting ‘State of the Art’ requirement

DALLAS--(BUSINESS WIRE)--The countdown is on and global businesses now have just six months until the General Data Protection Regulation (GDPR) is enforced. A recent study from Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, has found confusion among businesses about the regulations, with 30 percent unable to agree on what ‘State of the Art’ security requirements entail.

Trend Micro’s survey found wide variation on the definition of ‘State of the Art’ security among the 1,000 IT decision makers from businesses across the globe1.

- While 30 percent of businesses define it as buying security from an established market leader, another 17 percent think it means using products that pass independent third-party tests.
- Additionally, 16 percent believe it refers to products that are highly rated by analyst reports, and 14 percent think it covers start-ups providing innovative technology.
- Worryingly, 12 percent of IT decision makers are more concerned about the price of security products than whether the products they invest in meet GDPR requirements, and 9 percent were unable to provide a definition at all.

“There are many hurdles for businesses to overcome in establishing GDPR compliance – trying to demystify what ‘State of the Art’ means is but another challenge on the list,” said Rik Ferguson, vice president of security research for Trend Micro. “Regulatory enforcement bodies should offer further clarification on what ‘State of the Art’ means, so businesses can ensure they’re not stepping into a fine once May 2018 arrives.”

A Breach of Trust

Another hurdle for businesses to conquer involves the new timeline in regards to informing regional Data Protection Authorities, like the Information Commissioner’s Office (ICO) in the UK, and customers affected in the event of a data breach.

- Despite this, just 63 percent of businesses have a notification process in place for their customers. And, in countries like the US, there is a state-by-state approach requiring—or not—notification of a breach occurring.
- However, against GDPR guidelines, 21 percent of companies have a process to inform their data protection authority but actually avoid notifying customers.
- Companies are also not currently prepared to handle their customers’ ‘right to be forgotten,’ despite 63 percent citing that customers are asking for more transparency when it comes to the use of their data.
- While 77 percent have a process in place for data they collect, only 64 percent can process requests for data their partners collect.
- In addition, only 63 percent can process data their cloud service providers hold and 60 percent can fulfil requests relating to data third party agencies collect.

GDPR Purchasing Priorities

While mandating state of the art security does enable GDPR to maintain relevance in the face on continual technology advancement, the lack of specific approach definitions has introduced confusion and challenges around prioritization of technology.

- The most commonly implemented solution is intruder identification technology, with 34 percent incorporating it into their organization.
- Data leak protection (DLP) technology is also used by 33 percent of businesses, while 31 percent have started encrypting their data.
- Additionally, 29 percent are encrypting passwords or implementing hardware lockdowns to combat infected USB sticks.

Despite these cybersecurity purchases, this research reveals that the majority of organizations have not taken steps that would qualify their approach as state of the art, suggesting that they are depending on single purpose or legacy defences rather than taking a multi-layered approach.

To ensure data is as secure as possible, a layered cybersecurity defence must be implemented to ensure protection at every level of the IT environment.

However, it's not just about technology, as investing in education is also a GDPR priority. The research shows 63 percent of organizations have not yet started to raise awareness, and only 33 percent having introduced a new data protection policy.

"Educating employees and updating data protection policies is all well and good, but if corporate data isn't protected, intruders can't be detected, and if protections aren't in place to prevent data leaks, businesses don't have a cybersecurity strategy," Ferguson continued. "There's no silver bullet to cybersecurity; it's an all-encompassing war in which multiple techniques are necessary to fight hackers' increasing pragmatism. Any business that doesn't realize this quite simply won't be compliant with the regulation."

Trend Micro's market leading solutions for protecting users, servers, and networks, powered by XGen™ security, deliver a connected set of state of the art security technologies that can be used for GDPR compliance. They are designed to protect data wherever it is stored, whether physically, virtually, in the cloud or in containers, and are continually evolving in the same spirit as defined by GDPR and 'state of the art'.

To see Trend Micro's GDPR webinar, click here.
Is Your Security State of the Art? Click here for more information.

About the Research

For more information about Trend Micro's findings on the pulse of business leaders regarding GDPR, check out the infographic and supplemental blog post. In partnership with Opinium, Trend Micro conducted its GDPR survey between May 22 and June 28, 2017. The preceding results are gleaned from 1,132 online interviews with IT decision makers from businesses with 500+ employees in 11 countries, including United States of America (USA), United Kingdom (UK), France, Italy, Spain, Netherlands, Germany, Poland, Sweden, Austria and Switzerland. Respondents of the survey hold either senior executive, senior management or middle management positions in multiple industries including retail, financial services, public sector, media and construction.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks and endpoints. All our products work together to seamlessly share threat intelligence and provide a Connected Threat Defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

1 ITDMs from businesses with 500+ employees in 11 countries, including USA, UK, France, Italy, Spain, Netherlands, Germany, Poland, Sweden, Austria and Switzerland.

Contact:

Trend Micro Incorporated
Kateri Daniels, 817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2017-11-06-Trend-Micro-Study-Finds-State-of-the-Art-GDPR-Rule-Confuses-Businesses