Trend Micro Research Reveals C-level Executives Are Not Prepared for GDPR Implementation

•Senior executives shun GDPR responsibility in 57 percent of businesses
•42 percent of businesses don't know email marketing databases contain PII
•22 percent of businesses claim a fine 'wouldn't bother them' if found in violation

DALLAS--(BUSINESS WIRE)--With the General Data Protection Regulation (GDPR) taking effect May 25, 2018, businesses around the globe should be preparing accordingly. However, through a recent survey, Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, found that C-suite executives are not approaching the regulation with the seriousness required, resulting in overconfidence when it comes to compliance.

GDPR Awareness

The company's research reveals a robust awareness of the principles behind GDPR, with a strong 95 percent of business leaders knowing they need to comply with the regulation, and 85 percent having reviewed its requirements. In addition, 79 percent of businesses are confident that their data is as secure as it can possibly be. However, Gartner Inc. predicts that by May 25, 2018, less than 50 percent of businesses will not be in full compliance with GDPR requirements. The research company suggests organizations begin preparing now by focusing on five high-priority changes.

Despite this perceived awareness, there is some confusion as to exactly what Personally Identifiable Information (PII) needs to be protected. Of those surveyed, 64 percent were unaware that a customer's date of birth constitutes as PII. Additionally, 42 percent wouldn't classify email marketing databases as PII, 32 percent don't consider physical addresses and 21 percent don't see a customer's email address as PII, either. These results indicate that businesses are not as prepared or secure as they believe themselves to be. Regardless, this data provides hackers with all they need to commit identity theft, and any business not properly protecting this information is at risk of a penalty fine.

The Cost of Not Being Compliant

According to the survey, a staggering 66 percent of respondents appear to be dismissive of the amount they could be fined without the required security protections in place. Only 33 percent recognize that up to four percent of their annual turnover could be sacrificed. Additionally, 66 percent of businesses believe reputation and brand equity damage is the biggest pitfall in the event of a breach, with 46 percent of respondents claiming this would have the largest affect amongst existing customers. These attitudes are especially alarming considering businesses could be shut down in the event of a breach.

"Investing in state of the art equipment and employing data protection policies should be seen as a wise business practice, not an operational burden," said Rik Ferguson, vice president of security research for Trend Micro. "As a strategic security partner, we see it as our shared responsibility to help customers meet GDPR data security compliance."

Responsible Parties

Trend Micro also learned that businesses are uncertain as to who is held accountable for the loss of EU data by a U.S. service provider. Only 14 percent could correctly identify that the loss of data is the responsibility of both parties – 51 percent believing the fine goes to the EU data owner, while 24 percent think the US service provider is at fault.

In addition, it turns out businesses aren't sure who should take ownership of ensuring compliance with the regulation, either. Of those surveyed, 31 percent believe the CEO is responsible for leading GDPR compliance, whereas 27 percent think the CISO and their security team should take the lead. However, only 21 percent of those businesses actually have a senior executive involved in the GDPR process. Meanwhile, 65 percent have the IT department taking the lead, while only 22 percent have a board level or management member involved.

The Technology Required

With threats growing in sophistication, businesses often lack the expertise to combat them, and layered data protection technology is required. GDPR mandates that businesses must implement state-of-the-art technologies relative to the risks faced. Despite this, only 34 percent of businesses have implemented advanced capabilities to identify intruders, 33 percent have invested in data leak prevention technology and 31 percent have employed encryption technologies.

Trend Micro's commitment to GDPR compliance begins with its cross-generationalXGen™ security, which protects personal data throughout enterprises. Its solution is optimized for all environments where data may be stored, whether that's physically, virtually, on the cloud, or in containers. XGen is a strategy and platform spanning across all Trend Micro solutions, connected to alert and reporting data breaches as they happen. This approach provides businesses with the state-of-the-art tools mandated by GDPR.

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 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 over 5,000 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.

Contact:

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

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

Additional assets available online: Photos (2)

https://newsroom.trendmicro.com/2017-09-05-Trend-Micro-Research-Reveals-C-level-Executives-Are-Not-Prepared-for-GDPR-Implementation