Dell Survey Shows Organizations Lack Awareness and Preparation for New European Union General Data Protection Regulation (GDPR)
Tuesday, October 11, 2016 10:00:00 AM (GMT)

- More than 80 percent of global respondents know few details or nothing about GDPR
- Less than one in three companies feel they are prepared for GDPR today
- 97 percent of companies don't have a plan to be ready for GDPR
- Only nine percent of IT and business professionals are confident they will be fully ready for GDPR

Dell today announced results of a global survey on the European Union's new General Data Protection Regulation (GDPR), revealing that organizations – both SMBs and large enterprises – lack general awareness of the requirements of the new regulation, how to prepare for it, and the impact of non-compliance on data security and business outcomes.

Designed to strengthen protection of personal data for all EU citizens, the new regulation goes into effect in May 2018 and affects companies of all sizes, in all regions, and in all industries. Those not fully compliant when GDPR goes into effect risk significant fines, potential breaches and loss of reputation.

Survey results show that 82 percent of global IT and business professionals responsible for data security at both SMBs and enterprises are concerned with GDPR compliance. Although the majority of global IT and business professionals express compliance concerns, respondents lack general awareness of GDPR, and they are neither prepared for it now, nor expect to be when it goes into effect.

- More than 80 percent of respondents say they know few details or nothing about GDPR
- Less than one in three companies feel they are prepared for GDPR today
- Close to 70 percent of IT and business professionals say they are not nor don't know if their company is prepared for GDPR today, and only three percent of these respondents have a plan for readiness
- Respondents in Germany feel most prepared for GDPR (44 percent), while respondents in Benelux (Belgium, the Netherlands, Luxembourg) feel least prepared (26 percent)
- More than 75 percent of respondents outside Europe say they are not or don't know if they are prepared for GDPR
- Nearly all companies (97 percent) don't have a plan in place when GDPR kicks off in 2018

Results further show that while organizations realize failure to comply with GDPR will impact both data security and business outcomes, they are unclear on the *extent* of change required, or the severity of penalties for non-compliance and how changes will affect the business. Seventy-nine percent say they would not, or were not aware whether their organization would face penalties in its approach to data privacy if GDPR had been in effect this past year.

- Of the 21 percent of respondents who said they would face a penalty if GDPR were in place today, 36 percent think it would require only an easy remediation, or don't know the penalty
- Close to 50 percent believe they would face a moderate financial penalty or manageable remediation work
- Nearly 25 percent expect significant changes in current data security practices and technologies

Additional findings show that most organizations don't feel well-prepared across security disciplines for GDPR compliance.

- Less than half of respondents feel well-prepared for any of the security disciplines impacting GDPR
- Only 21 percent feel well-prepared for access governance, a key security discipline for GDPR

- More than 60 percent of enterprise respondents in Europe either are not or don't know if they are prepared for GDPR. Nearly 70 percent of SMB respondents in this region said they are not or don't know if they are prepared for GDPR
- More than 90 percent of respondents say their existing practices will not satisfy the new GDPR requirements
- More than 80 percent said they are well- or somewhat prepared with their organizations' current email security technologies
- Nearly 60 percent said they are well- or somewhat prepared with their organizations' current access governance technologies
- More than 80 percent said they are well- or somewhat prepared with their access management technologies
- 65 percent said they are well- or somewhat prepared with their next generation firewall (NGFW) technologies

Best practices help successfully address GDPR requirements and avoid the consequences of non-compliance

The EU GDPR was adopted by the European Parliament and Council this year, and becomes fully effective in 2018. Below are tips and strategies to help organizations adhere to security disciplines needed for GDPR regulations, so they can protect customer personal information, and avoid the data breaches, heavy fines and loss of reputation that may result from non-compliance:

- **Hire a data protection officer (DPO)**. A requirement for GDPR, the position can be full-time, or filled by an employee with other responsibilities or an outsourced agency. The good news is that a designated DPO can be used as a service, so some system integrators or resellers could offer this as a service to grow their businesses.
- **Deploy a firm access governance solution**. The ability to govern access to applications that permit access to EU citizens' personal data – particularly unstructured data – is a major factor in data security and GDPR compliance. Governance generally requires periodic review of access rights by line-of-business managers and attestation (or recertification) that the permissions align with their job roles and do not compromise data security. The One Identity family of Identity and Access Management solutions provides this level of visibility and control.
- **Control access management**. To satisfy GDPR, employees and contractors must have the correct access permission to do their jobs and nothing more. The right identity and access management technologies that facilitate this level of control include multi-factor authentication, secure remote access, risk-based/adaptive security, granular password management, and full control over privileged user credentials and activity.
- **Protect the perimeter**. Deploy next-generation firewalls to reduce the network's exposure to cyber threats, mitigate the risk of data leaks that could lead to a data breach resulting in stiff penalties assessed under GDPR, and deliver the forensic insight required to prove compliance and execute appropriate remediation following a breach. The Dell SonicWALL next-generation firewalls protect against emerging threats and feature deep packet inspection; real-time decryption and inspection of SSL sessions; adaptive, multi-engine sandboxing; and full control and visualization of applications.
- **Facilitate secure mobile access**. Foster the secure flow of covered data while enabling employees to access the corporate applications and data they need in the way they prefer, and with the devices they choose. Enhance data security (while removing access obstructions) by combining identity components, device variables and temporal factors (time, location, etc.) to deliver an adaptive, risk-based approach that ensures the right access all the time, every time, while concurrently improving data protection and GDPR compliance.
- **Ensure email security**. To fulfill GDPR requirements, achieve full control and visibility over email activity to mitigate the threat of phishing and other email-based attacks on protected information, while enabling the secure and compliant exchange of sensitive and confidential data.

Methodology

In the survey, conducted by Dimensional Research, 821 IT and business professionals responsible for data privacy at companies with European customers responded to questions about awareness, perception and readiness for GDPR, and the expected impact of non-compliance when GDPR comes into force in May 2018. The survey was conducted across the United States, Canada, Asia Pacific (Australia, Hong Kong, Singapore, India), United Kingdom, Germany, Sweden, Belgium, The Netherlands, France, Italy, Spain and Poland. Business executives at organizations with fewer than 100 employees also completed the survey.

Supporting Quotes:

John Milburn, vice president and general manager, Dell One Identity Solutions

“The European Union General Data Protection Regulation is the first update to European data protection laws since 1995, when the Internet was in its infancy and the constantly evolving cyber threats we know today did not exist. This survey reinforces the global lack of general understanding of GDPR, the scope of the regulation, and what organizations need to do to avoid stringent penalties. Results also show that while some organizations ‘think’ they are prepared, they will be in for a rude awakening if they experience a breach or must face an audit and are subject to the consequences of non-compliance with GDPR.”

Patrick Sweeney, vice president, product management and marketing, Dell SonicWALL

“This new regulation provides uniform data protection rights across the EU, and, to be in compliance, both European organizations and those outside of Europe that do business there must adopt an adaptive, user-centric, layered security model approach around the tenets of prevent, detect, respond and predict. To be GDPR-compliant, they need security solutions that enable them to prevent attacks, detect a potentially dangerous presence in their networks, respond quickly to that threat, and analyze and report on the health of their networks in real time.”

IDC

"Don't put off early consideration of GDPR by the two-year implementation period. The scale, complexity, cost and business criticality of GDPR means that it will take (at least) two years for most companies to achieve full compliance. Most companies need to start now."[1]

Supporting Resources:

- GDPR Global Survey
- **LinkedIn:** https://www.linkedin.com/groups/52461
- **Dell Software YouTube:** www.youtube.com/user/DellSoftwareVideo
- **Dell Security Solutions:** https://security.dell.com/
- **Twitter:** https://www.twitter.com/SonicWALL and https://www.twitter.com/OneIdentity
- **Facebook:** https://www.facebook.com/sonicwall

[1] “Executive Brief on GDPR: A Primer for Getting Started Towards Compliance,” by Duncan Brown, IDC, March 2016

Dell Technologies

Dell Technologies is a unique family of businesses that provides the essential infrastructure for organizations to build their digital future, transform IT and protect their most important asset, information. The company services customers of all sizes across 180 countries – ranging from 98 percent of the Fortune 500 to individual consumers – with the industry’s most comprehensive and innovative portfolio from the edge to the core to the cloud.

Dell EMC World

Join us Oct. 18-20 at Dell EMC World 2016, Dell Technologies’ flagship event bringing together technology

and business professionals to network, share ideas and help co-create a better future. Learn more at www.dellemcworld.com and follow #DellEMCWorld on Twitter

Dell is a trademark of Dell Inc. Dell disclaims any proprietary interest in the marks and names of others.

View source version on businesswire.com: http://www.businesswire.com/news/home/20161011005445/en/

--30-- SEG/DA

Contact:

Dell, Inc.
Media Contact:
Jennifer Bernas, 949-790-9855
Jennifer_Bernas@dell.com
or
Analyst Contact:
Beth Johnson, 415-412-6891
Beth_Johnson@dell.com

Industries: Technology, Data Management, Networks, Software, Security
Languages: English
Primary Identifiers: DELL-US
Related Identifiers: DELL-US
Source: Dell Technologies
Subjects: Conference, Survey, Product/Service, Trade Show