MARSH

全球网络风险认知调查报告 | 2017年10月

《欧盟数据保护条例》生效在即，企业是否做好准备：衡量网络风险管理的指标之一

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

《欧盟数据保护条例》生效在即，企业是否做好准备：衡量网络风险管理的指标之一

目录

1 调查结果概述

2 部分企业对于《欧盟数据保护条例》的生效做了更加充分的准备

3 一部欧洲的法规，却具有全球性影响

4 鼓励企业加强网络风险管理

8 《欧盟数据保护条例》合规并不意味着网络风险管理做的出色

10 加强网络风险管理的良机随之而来

12 调查方法 / 受访者情况

调查结果概述

对于《欧盟数据保护条例》合规而言，网络风险管理既是因也是果。

《欧盟数据保护条例》是当今隐私保护法经历的一次最重大的修订，它的出台将使欧洲的数据和隐私保护规则发生巨大变化。该条例不仅针对在欧盟开展经营的企业应如何管理和保护个人数据做了严格的规定，还赋予欧盟个人更高的隐私权（无论他们居住在哪里皆如此）。《欧盟数据保护条例》还带来了增长和创新的动力，鼓励在欧盟经营的企业实施更加严格的数据保护并更新经营方式，以适应数据驱动型环境的需要。因此，虽然新规并未提及，但是遵守《欧盟数据保护条例》还会产生一个最显著的连锁效应，那就是管理和应对网络风险演变的能力将得到提升。

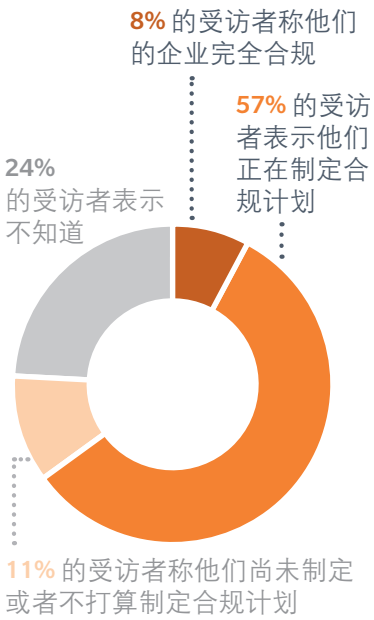
我们近期进行的一项调查也印证了这两者之间的密切关系。来自全球多个行业的1300多名企业高级管理人员参加了此次调查。与尚未开始制定合规计划的受访者相比，那些声称其公司正在制定计划或者完全符合新规的受访者表示其会采取某些网络安全措施的可能性要高出两倍多，而会采取某些网络应变能力措施的可能性则要高出三倍多。面对《欧盟数据保护条例》即将生效，准备更加充分的受访者表示他们的企业购买或强化网络风险保险的可能性是其他受访者的1.5倍多，这将有助于抵消网络风险事件的财务影响(见图表1)。

图表 1

《欧盟数据保护条例》合规与网络风险管理之间存在密切联系。

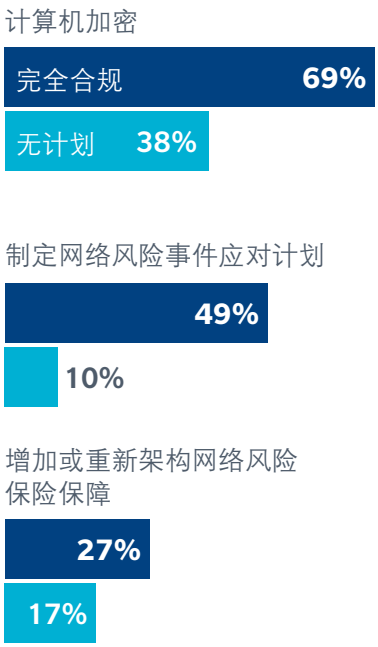
在《欧盟数据保护条例》管辖的企业中，有2/3正在进行合规准备或者能够满足新规要求。

问：贵公司在《欧盟数据保护条例》合规/合规准备方面进展如何？



一些企业利用《欧盟数据保护条例》合规的契机来强化某些关键的网络风险管理做法。

问：贵公司在过去12-24个月内采取了哪些措施？



对于《欧盟数据保护条例》合规而言，网络风险管理既是因也是果。拥有强大网络安全措施的企业在合规方面占有先机，因为《欧盟数据保护条例》大力鼓励某些做法，例如加密措施。同样，网络风险事件规划和投保网络保险等做法在《欧盟数据保护条例》中虽未有明确要求，但有助于企业快速调动资源，以满足《欧盟数据保护条例》中关于72小时数据泄露通知的要求。《欧盟数据保护条例》还会推动网络风险应对准备工作：条例中的某一主要条款指出，适当的技术和组织架构措施是确保风险得到妥善防护的基础。

那么，企业在《欧盟数据保护条例》合规方面的进展如何呢？在《欧盟数据保护条例》所管辖企业的受访者中，只有8%的人表示他们的企业完全合规，57%的人称他们的企业正在着手制定合规计划，而11%的人表示他们的企业尚未采取行动。由于做到合规耗时耗力，因此到2018年5月《欧盟数据保护条例》正式生效时，许多企业将面临合规方面的挑战。

然而，《欧盟数据保护条例》也具有积极的影响。仅应对准备一项就可以促使管理层关注更多数据和隐私保护问题并刺激相关投入。在那些对《欧盟数据保护条例》准备更加充分的受访者中，有78%的人表示他们会增加网络风险管理支出，包括网络风险保险支出。

聚焦

部分企业对于《欧盟数据保护条例》的生效做了更加充分的准备

距离《欧盟数据保护条例》正式生效只剩下几个月的时间了，然而仅有8%的受访者表示他们的企业完全合规，将近1/3的受访者（32%）称他们的企业尚未制定合规计划或者不清楚其企业是否已经拥有相关计划。为什么会这样呢？

其中一个可能的原因就是企业规模。大致来说，较大型企业更有可能满足《欧盟数据保护条例》的合规要求（见图表2）。这些企业可以投入更多资源和管理设施，从而为合规提供支持。许多此类企业还在美国设立了重要运营机构，而美国在数年前就出台并实施了严格的数据保护和泄露通知政策。因此，这些企业占有先机，他们很可能已经拥有了严格的合规体系，更容易满足《欧盟数据保护条例》的要求。

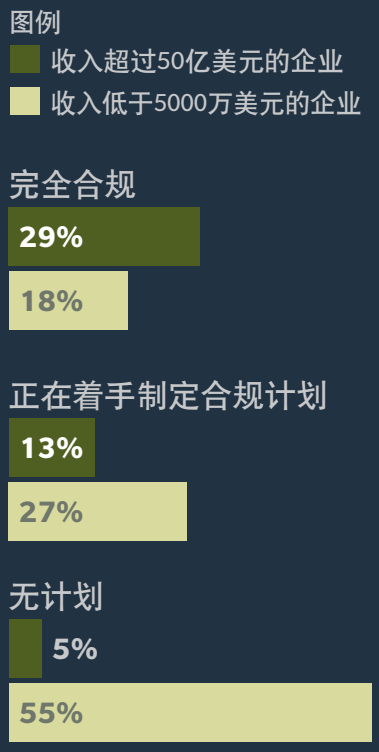
除企业规模外，还存在很多其他因素。一些企业可能因为应付手头任务而分身乏术。《欧盟数据保护条例》要求企业不应仅仅满足于符合规定，还应重新思考数据管理做法。这种更加全面的方法需要企业在管理上投入更多精力和资源，关注新规对企业的影响、哪些行为可能引起法律责任以及新规与网络风险保险和其他合规要求之间的关系。

另外，许多企业，特别是那些自认为在传统意义上并不属于数据收集行业的企业，可能并不十分清楚自己应当遵守《欧盟数据保护条例》。举例来说，汽车和化学制造企业所做的准备要少于其他行业的企业。然而现实情况是，当今的任何企业都属于数据驱动型企业。即使那些并不直接收集、持有或分析客户数据的企业也会发现，他们可能会因为关键供应商遭到网络攻击而受到严重影响。

最后，《欧盟数据保护条例》中的很多细节问题还有待各国监管机构做出澄清和说明。因此，那些对《欧盟数据保护条例》合规流程做了深入研究的企业的受访者并不倾向于说自己的企业能够做到完全合规，而那些尚未开始制定合规计划的企业的受访者可能正在等待监管机构的说明和澄清。

图表 2 规模越大的企业对《欧盟数据保护条例》所做的合规准备工作越充分。

问：贵公司在《欧盟数据保护条例》合规方面取得了哪些进展？



一部欧洲的法规，却具有全球性影响

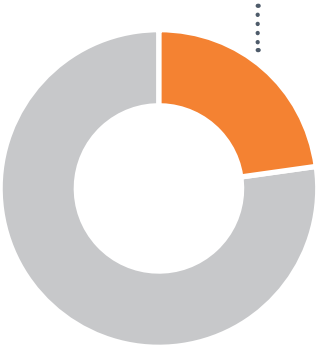
当前，几乎每家企业都会涉及数据的收集、分析和使用工作。这带来了无限的潜在机遇，但信息被不当使用或落入坏人之手的风险也随之而来。由于网络攻击分子的手法越来越娴熟，用户数据保护需求正在急剧增加。现在的问题不是企业是否会受到网络攻击，而是网络攻击何时会发生。的确我们在调查中也发现，在《欧盟数据保护条例》管辖的企业中，有23%在过去一年曾经遭受过网络攻击（见图表3）。

为了加强对欧盟公民个人隐私的保护，《欧盟数据保护条例》要求持有或使用个人数据的企业采取必要的防范措施。该条例旨在对当前的数据保护规定进行更新，鼓励企业采取更加严格的数据管理措施，要求企业在遭受数据损失时执行更加严厉的数据泄露通知规定。然而，《欧盟数据保护条例》还具有更加广泛的影响。为什么呢？

图表 3 现在的问题不再是企业是否会受到攻击，而是网络攻击何时会发生。

问：贵公司在过去12个月是否遭受过网络攻击？

在《欧盟数据保护条例》管辖的企业中，有23% 在过去一年曾经遭受过网络攻击。



首先，《欧盟数据保护条例》做出的明确要求相对较少，但最终各国监管机构可能会提供更多指导。截至目前，只有少量条款对具体行为做了规定，例如企业应于个人数据发生泄露后72小时内通知监管机构或者大力鼓励企业采取加密措施。这种只提原则的方法要求企业根据自身风险状况确定合适的管控措施。虽然《欧盟数据保护条例》没有给出现成的核对清单，但是要求企业综合考量自身业务运营情况并重新审查如何保护个人数据。满足《欧盟数据保护条例》的合规要求与管理网络风险不仅存在差异，还具有无法割舍的联系。

其次，《欧盟数据保护条例》的管辖范围是跨地域的，适用于所有收集或处理欧盟居民数据的企业，无论这些企业的总部位于哪里或者在哪里开展运营皆如此。任何在欧盟范围内从事产品或服务活动的公司都可能受到影响。

再次，违规企业将受到严厉制裁。政策制定者希望通过罚款的办法加强合规，罚金金额之高是史无前例的，可能高达企业全球营业额的4%或者2000万欧元，以两者之中较高者为准。根据奥纬的研究表明，仅英国一个国家，富时100指数（FTSE100）企业在第一年1受到的处罚就可能超过60亿美元。

换言之，《欧盟数据保护条例》将企业的注意力转移至数据保护和网络风险管理上，将产生深远的影响。作为起草者的Jan Philipp Albrecht表示，《欧盟数据保护条例》不仅将“改变欧洲的数据保护法规，还将影响到全球范围”。

《欧盟数据保护条例》：简介

《欧盟数据保护条例》已于2016年5月24日颁布，实施过渡期为2年。所有收集欧盟公民数据的企业（不仅限于欧盟公司）都受到影响，违者将被处以2000万欧元或全球营业额4的罚款，以两者之中较高者为准。其它要点内容包括：

- 收集特定类型的个人敏感信息需要征得明确同意。
- 对数据主体画像提出了新的限制条件。
- 企业必须检查哪些环节涉及到个人数据并表明自己符合规定。
- 当核心活动中包含对特殊个人数据和/或刑事定罪信息进行大规模处理或者对数据主体实施系统性监控时，企业应指定一名数据保护专员。
- 提供某些新的产品或服务或者更新某些产品或服务时，应进行数据隐私保护影响评估。
- 发生个人数据泄露时，企业应在不晚于72小时内通知监管机构和数据主体，不得无故拖延。
- 数据主体被赋予更多、更大的权利，包括有权要求对个人数据进行访问、校正和删除。
- 拥有单一的牵头监管机构，开展统一的执法行动。

鼓励企业加强网络风险管理

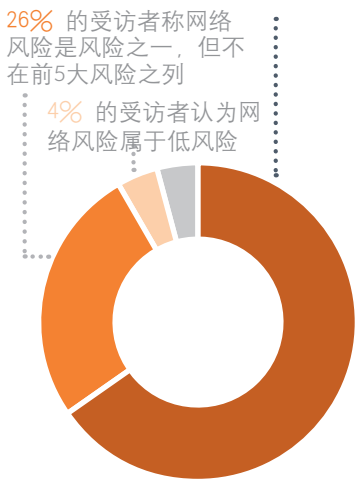
《欧盟数据保护条例》的合规要求使网络风险管理跃居企业日程的首要位置。在来自《欧盟数据保护条例》所管辖企业的受访者中，有65%的人将网络风险列为其企业应优先管控的前5大风险之一。只有4%的受访者认为网络风险为低风险或者不属于优先管控的风险（见图表4）。

然而，认知和行动之间是有差距的。我们的数据表明，满足新规要求与加强网络风险管理之间存在关联性。那些着手准备应对《欧盟数据保护条例》合规要求或者做到合规的企业不仅在增加网络风险管理开支上的可能性高于那些尚未开始制定合规计划的企业，前者是后者的1.5倍多，而且从总体上说这些企业在网络风险管理方面也已经采取了更多的措施（见图表5）。

图表 4

受到《欧盟数据保护条例》管辖的大多数企业都将网络风险视为应当优先管控的重点风险。

问：在贵公司的风险管理重点中，网络风险属于…



其余受访者回答“不清楚”

图表 5

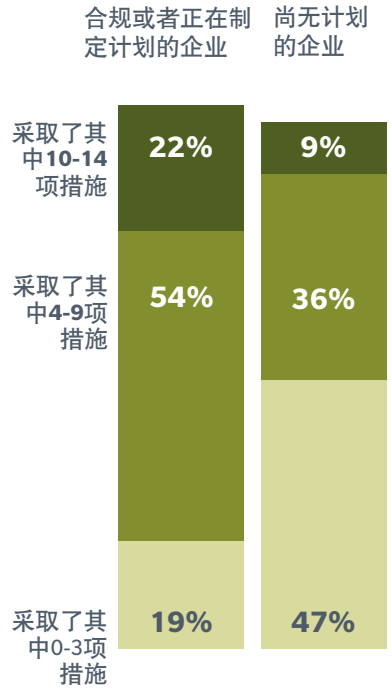
与那些尚无计划的企业相比，正在着手应对《欧盟数据保护条例》合规要求的企业在网络风险管理方面投入了更多资源并采取了更多措施。

正在着手应对《欧盟数据保护条例》合规要求的企业中有超过3/4已经增加了开支…

问：我预计未来12个月本公司在网络风险管理方面的投资会…

在调查列出的14项网络风险管理措施中，大多数企业采纳了其中至少4项。

问：贵公司在过去12–24个月采取了下列哪些措施？



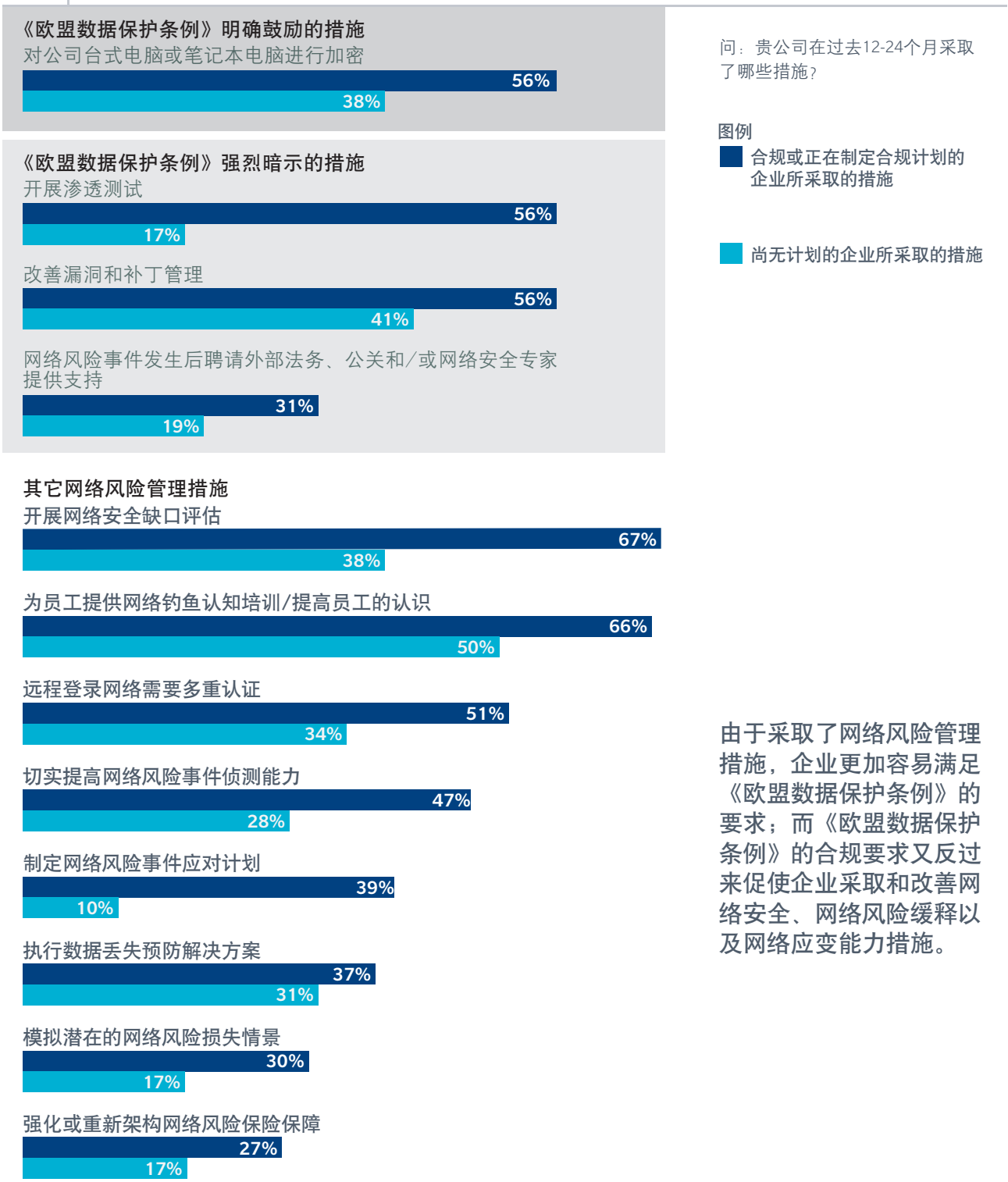
不知道/其它没有显示的回答

我们要求受访者从一系列网络风险管理措施中做出选择，这些措施从使用网络风险评估工具到实施网络安全和网络风险保险战略再到开发网络风险应变能力流程不等。在“着手准备企业”以及“合规企业”小组中，大约75%的受访者表示他们的企业在过去12-24个月采取了4项以上措施；而在“尚未着手准备企业”小组中，选择4项以上措施的受访者只有45%。

那么，企业对哪些网络风险管理措施进行了投资（见图表6）？

图表 6

《欧盟数据保护条例》合规的企业或者正在制定合规计划的企业采取网络风险管理的可能性更高。



由于采取了网络风险管理措施，企业更加容易满足《欧盟数据保护条例》的要求；而《欧盟数据保护条例》的合规要求又反过来促使企业采取和改善网络安全、网络风险缓释以及网络应变能力措施。

在我们列出的信息安全措施中，只有一项 – 即公司电脑加密 – 是《欧盟数据保护条例》明确鼓励的。正在着手准备应对《欧盟数据保护条例》或者完全合规的企业对这项措施的采纳程度也非常高，有 56%的受访者表示他们公司在过去两年中对电脑系统进行了加密。相比之下，在尚未开始合规流程的企业中，这一比例只有38%。

其中一个原因就是近年来云计算技术的广泛应用。越来越多的企业开始将关键数据迁移至云端，作为云流程的组成部分，他们需要主动对数据进行识别和归类。这为企业满足《欧盟数据保护条例》合规要求创造了先机。另外，《欧盟数据保护条例》要求的许多安全控制措施与其他数据保护标准（例如ISO 27018云端隐私保护标准）类似。事实上，正如我们调查所发现，在“合规”或“着手准备”小组、已对数据进行了加密的企业中，有超过85%使用了云服务（见图表7）。

除公司电脑加密以外，还有几项网络风险管理措施也被广泛采用，包括渗透测试、改善漏洞和补丁管理以及使用外部危机管理服务（对于及时缓释风险和及时发送数据泄露通知是必要的）。虽然《欧盟数据保护条例》对这些措施未做明确要求，但却强烈暗示企业有必要采取这些措施。

毫无意外，在“着手准备应对《欧盟数据保护条例》”或者“满足《欧盟数据保护条例》合规要求”的企业中，在过去两年中采取了所有措施的超过半数。然而在尚未制定合规计划的企业中，这一比例只有大约1/4。

总体而言，我们发现被采纳程度最高的网络风险管理措施都是以防护为主的网络安全措施。例如，在“着手准备应对《欧盟数据保护条例》”或者“满足《欧盟数据保护条例》合规要求”的企业中，有67%进行了网络安全缺口分析，有56%开展了渗透测试，有66%为员工提供或强化了网络钓鱼认知培训。

由于网络风险管理在以前被视为IT部门的工作（73%的受访者认为IT部门是第一责任人），因此大多数公司都注重通过技术安全措施来预防网络风险事件的发生，而不是采取措施，在网络风险事件发生时帮助企业做出响应。然而，许多拥有完善风险管理计划的企业会从经济的角度审视这一风险。他们采用全面的方法，将网络风险保险和网络应变能力规划与传统的隐私风险缓释和信息安全措施结合起来，进而获得最大程度的保护。

在《欧盟数据保护条例》合规方面取得最大进展的企业更有可能共享这一理念。举例来说，“着手准备应对《欧盟数据保护条例》”或者“满足《欧盟数据保护条例》合规要求”的企业购买网络风险保险的可能性大约是那些尚无计划的企业的两倍。同样，

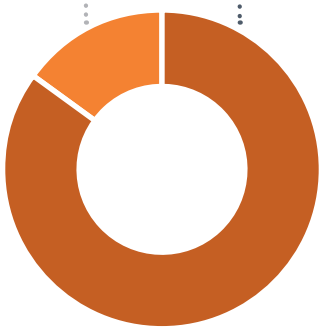
图表 7

使用云服务可能是给数据加密的一种有效方法。

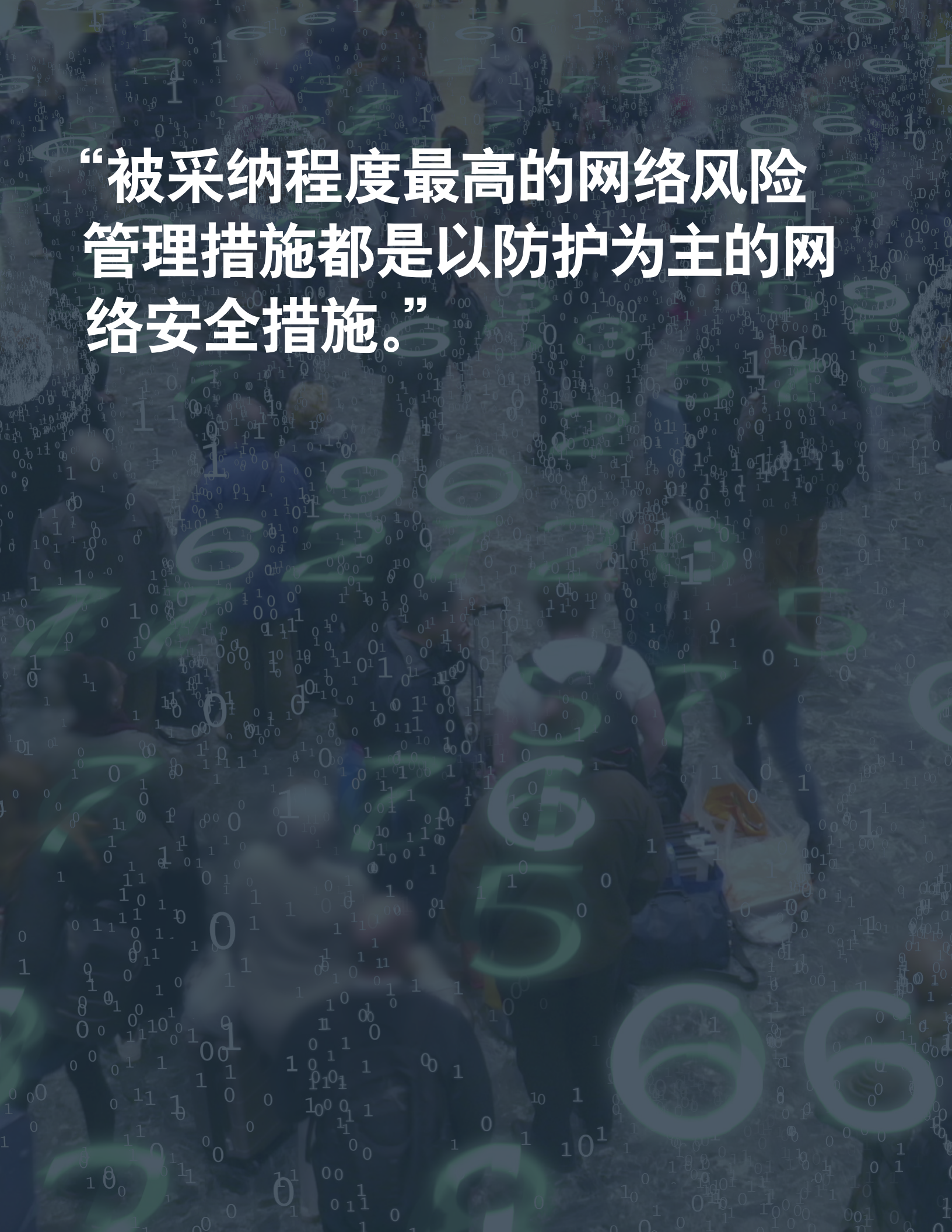
问：贵公司在过去12-24个月是否对电脑进行了加密？如果是，贵公司是否使用了云服务？

在“着手准备应对《欧盟数据保护条例》”或者“满足《欧盟数据保护条例》合规要求”并且已对数据进行了加密的企业中，有85%也使用了云服务。

其余15%的企业没有使用云服务。



自认为正在着手准备或者合规的企业与同行进行网络风险同比评估的可能性高出1.4倍，而制定网络风险事件应对计划的可能性则高出3.9倍。



“被采纳程度最高的网络风险管理措施都是以防护为主的网络安全措施。”

《欧盟数据保护条例》合规并不意味着网络风险管理做的出色

尽管对象可能存在重叠，但是满足《欧盟数据保护条例》的合规要求并不等同于网络风险管理做的出色。部分受访企业即使已经对《欧盟数据保护条例》做了较为充分的准备且采取了诸多最佳做法，也可能无法在网络风险管理方面称得上完全准备就绪。

让我们来看看网络风险管理工具的使用情况。在声称其企业正在着手准备应对《欧盟数据保护条例》或者完全合规的受访者中，只有53%的人表示他们已经对网络风险损失的财务影响进行了评估。量化风险有助于提高精确度，使风险管理决策变得更加有效（见图表8）。

但是在此类受访者中，只有24%的人称他们的企业会定期使用可量化的术语对网络风险保险进行表述。大多数企业依赖定量指标 – 交通灯中的红、黄、绿色 – 说明风险的严重程度。随着网络风险数据标准化程度的不断提高，越来越多的企业在风险量化中遇到的挑战将逐步降低。

在关键网络风险管理措施的采用方面，同样存在差异。例如，在着手准备应对《欧盟数据保护条例》或者完全合规的受访者中，有56%的人称他们对电脑进行了加密。这说明，其余44%的受访者或者不清楚他们的电脑系统是否加密或者还没有采取加密行动。同时，受访者表示他们较少采用比较昂贵复杂的措施，例如减少外部系统连接。显然，任何一种措施的采用率都不可能达到100%。

网络风险保险是另外一个存在改善空间的领域。在着手准备应对《欧盟数据保护条例》或者合规的受访者中，只有65%的人表示他们的企业购买了网络风险保险或者在未来12个月内打算投保这一保险，大约12%的人表示他们的企业没有购买或不打算购买网络风险保险。

从地区的角度看，网络风险管理措施的采用情况更是参差不齐。举例来说，美国的网络风险保险措施采用率相对较高，监管机构要求进行数据泄露通知是主要原因所在。在全球其他地区，采用网络风险管理措施的步伐则相对缓慢。

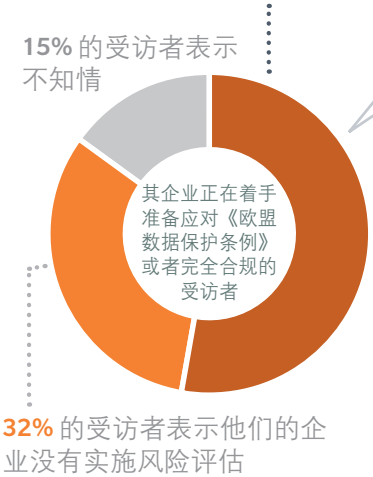
我们相信，《欧盟数据保护条例》的合规要求可能会促使网络风险措施在更大范围内得到采用。这是因为，《欧盟数据保护条例》中包含一个主要条款，规定企业一旦获悉欧盟公民的个人数据发生泄露，应在72小时内通知监管机构和受到影响的数据主体，不存在任何例外情况。企业似乎会严格遵守这一要求，根据我们的调查显示，在“《欧盟数据保护条例》合规”的企业中，有98%称他们拥有数据泄露通知计划。

数据泄露通知计划不仅会产生高额费用，执行起来也比较复杂。网络风险保险可以承保相关费用，当发生数据泄露时，能够帮助企业快速获得危机管理、法务、公关以及网络取证领域的优秀公司的帮助。因此，虽然法律未做明确要求，网络风险保险仍然是一种实用的解决方案。

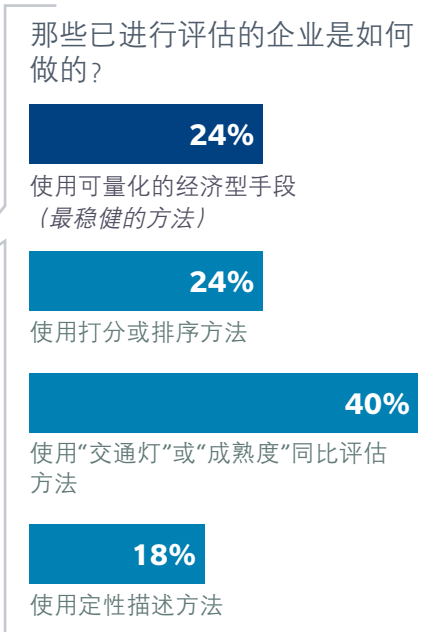
图表 8

在着手准备应对《欧盟数据保护条例》的企业中，只有半数企业进行了财务影响评估，而使用稳健评估方法的企业数量则更少。

问：贵公司是否对网络风险事件可能造成的最坏财务后果进行了评估？



问：贵公司如何评估网络风险？*（多项选择，选项没有全部显示）*



图表 9

企业仍有可能受到第三方风险的影响。

在满足《欧盟数据保护条例》合规要求或者正在着手制定合规应对计划的企业中，虽然有67%表示他们对第三方风险进行了评估，但是在如何评估和管理风险这一点上，仍然存在不足。

问：贵公司采取了哪些措施来评估和管理由供应商及其他第三方带来的网络风险？

17%

分析他们的财务实力，确保他们有能力做出赔偿

20%

在合同中约定好网络风险损失责任限额

20%

对供应商的网络安全状况实施持续监控

24%

评估他们的网络安全状况/或要求提供单独证明

34%

审查供应商关系及其数据访问权限

最后，即使企业采取了一切措施保护其网络安全，他们仍有可能受到来自第三方的威胁。在企业做了较为充分准备的受访者中，大约67%的人称他们对外部供应商带来的网络风险进行了评估。然而，细节才能说明问题。在上述受访者中，只有34%的人称他们的企业对供应商关系以及供应商的数据管理权限进行了审查，只有20%的人表示他们的企业会检查或持续监控供应商的网络安全状况（见图表9）。

加强网络风险管理的良机随之而来

企业应以《欧盟数据保护条例》合规为契机来加强网络风险管理

截至2018年5月做到《欧盟数据保护条例》合规是企业上下面临的一项挑战，耗时耗力并需要运用工具、流程和专业知识。企业的隐私保护和数据管理做法也可能需要做出重大变更。距离《欧盟数据保护条例》正式生效还有不到一年的时间，有2/3的受访者表示他们的公司仍在着手准备新规的合规工作 – 甚至有的企业尚未采取行动。

然而，将注意力放在尽早满足《欧盟数据保护条例》的合规要求上固然重要，却容易忽视合规努力所具有的更广泛的影响。在很多企业中，《欧盟数据保护条例》已成为一个引爆点，不仅会推动高层管理者关注具体的数据或隐私保护工作，还会促使他们对网络风险管理进行更加广泛、更具战略性的审视。毕竟，正如《欧盟数据保护条例》所述，网络安全准备情况是确定一家企业是否采取了“适当的技术和组织架构措施”的基础。但是如我们的调查所示，准备最充分的企业会从新规中明确提出的网络安全要求出发，采取更多的网络风险管理最佳做法。

目前，要做的工作还很多，改善空间也很大。但是，为什么有些企业会取得较大进展呢？

首先，他们知道网络风险管理工作应由各部门分担，从IT部门到高级管理层都需参与进来。无论规模多大，许多此类企业都设立了内部跨部门工作组或者指导委员会，由高级管理人员牵头（有时包含CEO在内），有时还要向 CEO汇报。这些企业充分利用《欧盟数据保护条例》合规的机会，对企业如何收集、保存、使用和管理数据实施全方位的审查。他们运用新的工具，例如云服务；保护隐私权；并做了大量投资，确保他们所处理的信息得到安全保护。另外，他们还重新检查自己的隐私和数据保护做法，确保他们的人员、流程和技术能够符合要求。

其次，他们承认网络风险事件发生的必然性。他们不仅重视预防网络攻击，还能够快速应对网络风险事件并减少潜在损失。他们将满足《欧盟数据保护条例》提出的数据泄露通知要求视为一个机会，藉此制定更加有力的事故管理流程 - 这意味着他们或者会购买网络风险保险、聘请危机管理专家；或者实行电脑系统加密，使被盗信息作废。

最后，他们采取定量和全面的方法。要符合《欧盟数据保护条例》的规定，企业需执行与其潜在风险相适应的措施，前瞻性企业都会准确分析他们的风险状况（内部和外部风险）并为潜在损失预留准备金。因此，他们不仅会投资部署合适的网络安全防护措施，还会强化网络风险事件应对计划以及其他风险缓释和应变能力措施。

换言之，这些企业将《欧盟数据保护条例》合规视为一个具有转折意义的机会。在准备应对新规的过程中，他们提升了自己的网络风险管理水平，并将通常意义上的束缚转化为竞争优势。

“在很多企业中，《欧盟数据保护条例》已成为一个引爆点，不仅会推动高层管理者关注具体的数据或隐私保护工作，还会促使他们对网络风险管理进行更加广泛、更具战略性的审视。”

调查方法

2017年7-8月，达信与微软联合进行了全球网络风险认知调查。本报告是基于此次调查的结果撰写而成。

总的来说，共有1312名高级管理人员参加了此次全球调查活动，他们来自多个关键职能岗位，包括信息技术、风险管理、财务、法务/合规、高级管理以及董事会等。

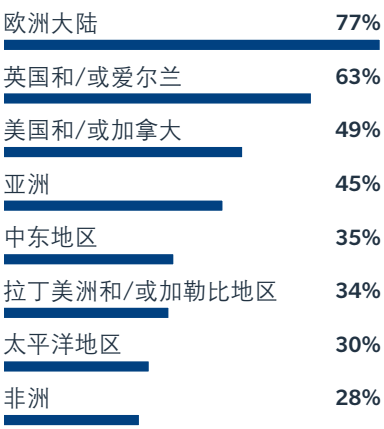
在受访者中，有41%的人来自《欧盟数据保护条例》管辖的企业。我们提问了一系列问题，并了解了受访企业从事哪些经营活动以及是否向欧盟成员国居民提供产品或服务，得出了这一结论。

来自《欧盟数据保护条例》管辖企业的受访者共有537人，均匀分布于8个地区，涉及行业超过25个。在这些受访者中，有15%的人是IT专业人士，有26%的人来自风险管理岗位，有7%的人属于法务合规人员，有29%的人来自其他岗位。受访者中还包括307名最高层管理人员。

受访者情况

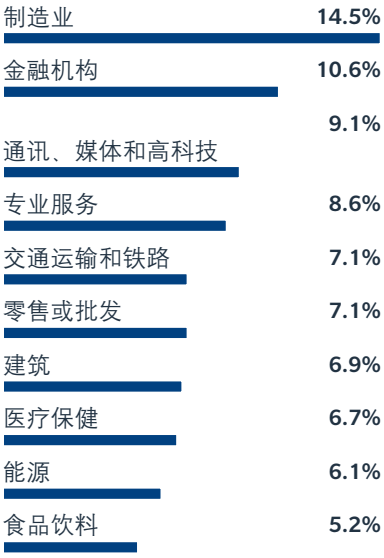
营业地区

537名受访者来自《欧盟数据保护条例》管辖的企业。这些企业向下列地区提供产品或服务：

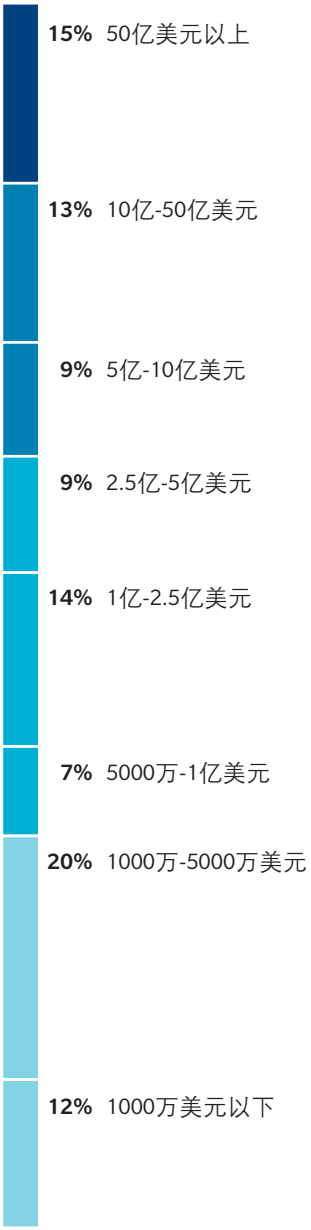


行业分布

来自《欧盟数据保护条例》管辖企业的受访者主要分布于以下行业：



收入情况（美元）



尾注

[1]http://www.oliverwyman.com/media-center/2017/may/ftse-100-companies-could-face-up-to-p5-billion-a-year-in-fines-w.html

关于达信

达信是全球领先的保险经纪和风险管理专家，通过确定、设计和提供创新型解决方案帮助客户有效管理风险并取得成功。达信在全球拥有约30000名员工，向全球130多个国家和地区的客户提供建议和服务。达信是Marsh & McLennan Companies（纽交所代码：MMC）的全资子公司，后者是一家全球性专业服务公司，向客户提供风险、战略和人力资源服务。Marsh & McLennan Companies在全球拥有大约60000名员工，年收入达130亿美元，旗下子公司还包括：佳达，风险和再保险中介服务领域的领先企业；美世，人力资源、健康福利、退休方案以及投资咨询领域的领先企业；奥纬，管理咨询领域的领先企业。请在推特关注@MarshGlobal，并在新浪微博关注@达信Marsh，或者在微信公众号搜索MarshChina关注达信微信公众平台，或者订阅BRINK获取相关信息。

达信是Marsh & McLennan Companies的子公司，后者也是佳达、美世和奥纬的母公司。

MARSH