数据安全的冰与火之歌

从GDPR看企业数据安全合规建设

李睿

Jul. 2018

演讲嘉宾介绍

李睿 Lisa Li

风险与控制服务

合伙人

背景

- Lisa有超过18年IT管理和技术经验。 近10年她主要从事美国上市互联网公司的IT审计和风险控制工作，覆盖了搜索、电商、游戏、OTA、视频、新闻门户、社交媒体等主要互联网细分行业
- 作为IT风险和信息安全的专家，她多年来专注于业务安全规划、业务战略与IT和安全的承接、安全技术架构、安全治理和合规、IT风险和控制、数据防泄漏、安全运营等，协助银行、保险、能源、电信、高科技、互联网等的不同企业应对业务及网络安全风险，建立长效的安全保障能力
- 她目前研究的领域包括数字风险保障、互联网业务安全、数据防泄漏、业务连续性、云安全和移动安全,致力于帮助企业建立可信的网络空间

经验

- 在线业务风险管控：**通过多年互联网公司的IT风险保障和控制经验，识别和分析互联网风险，帮助企业管理互联网环境下的在线风险、网络风险和IT风险**
- 安全战略与规划： 协助中国大型企业制定中长期安全战略和路径规划，尤其是控制业务转型中的IT风险，建立更前瞻更可信的安全战略和安全体系
- 数据防泄漏： 帮助企业从业务出发，梳理高价值数据和资产，识别数据泄漏风险，尤其是在云或者移动环境下的安全风险，建立数据安全保护策略和机制，结合DRM、DLP、加密等技术方案，保护企业客户信息、研发信息、市场和销售数据等核心数据
- 安全运营：帮助企业形成整体安全视图，与企业一起通过安全分析、威胁情报、事件响应，建立动态整合的安全运营和响应体系。部署安全运营中心(SOC)，优化安全信息管理和网络监控
- 业务连续性与IT灾备：主要包括业务连续性体系建设、业务影响性和风险分析、应急预案和演练、应急管理、IT服务持续性管理、组织架构搭建和制度建设、灾备中心建设规划等工作，帮助企业在日趋复杂的业务和IT环境中增强灾难和突发事件的处置能力

电话： 010-6533-2312

136-6117-5575

E-mail：
Lisa.ra.li@cn.pwc.com

Master in Computer Science, University of Denver, USA
美国丹佛大学 计算机硕士

Certified Information Systems Auditor (CISA)
注册信息系统审计师

Certified Information Security ISO27001 Lead Auditor
注册信息安全审核员

Certified Business Continuity Professional (CBCP)
注册业务连续性专家

Certified Project Management Professional (PMP)
注册项目管理专家

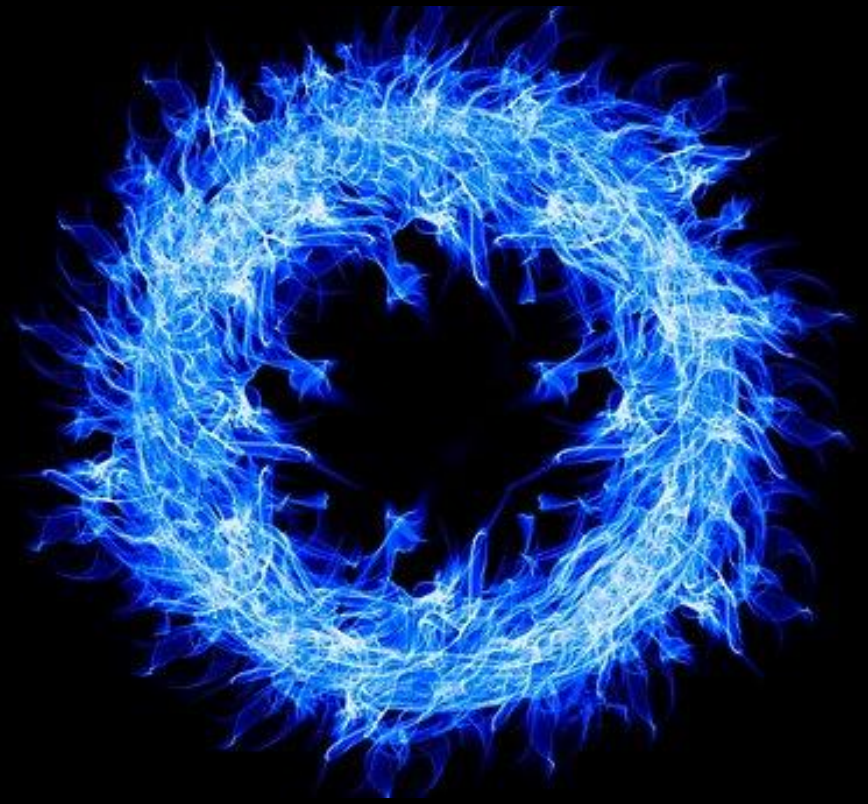
Certified ITIL v3 Professional
注册ITIL V3专家

Certified Advanced Java Developer
高级JAVA工程师

Certified Advanced Perl Developer
高级Perl工程师

OSAC（Overseas Security Advisory Council)
执行委员会 成员

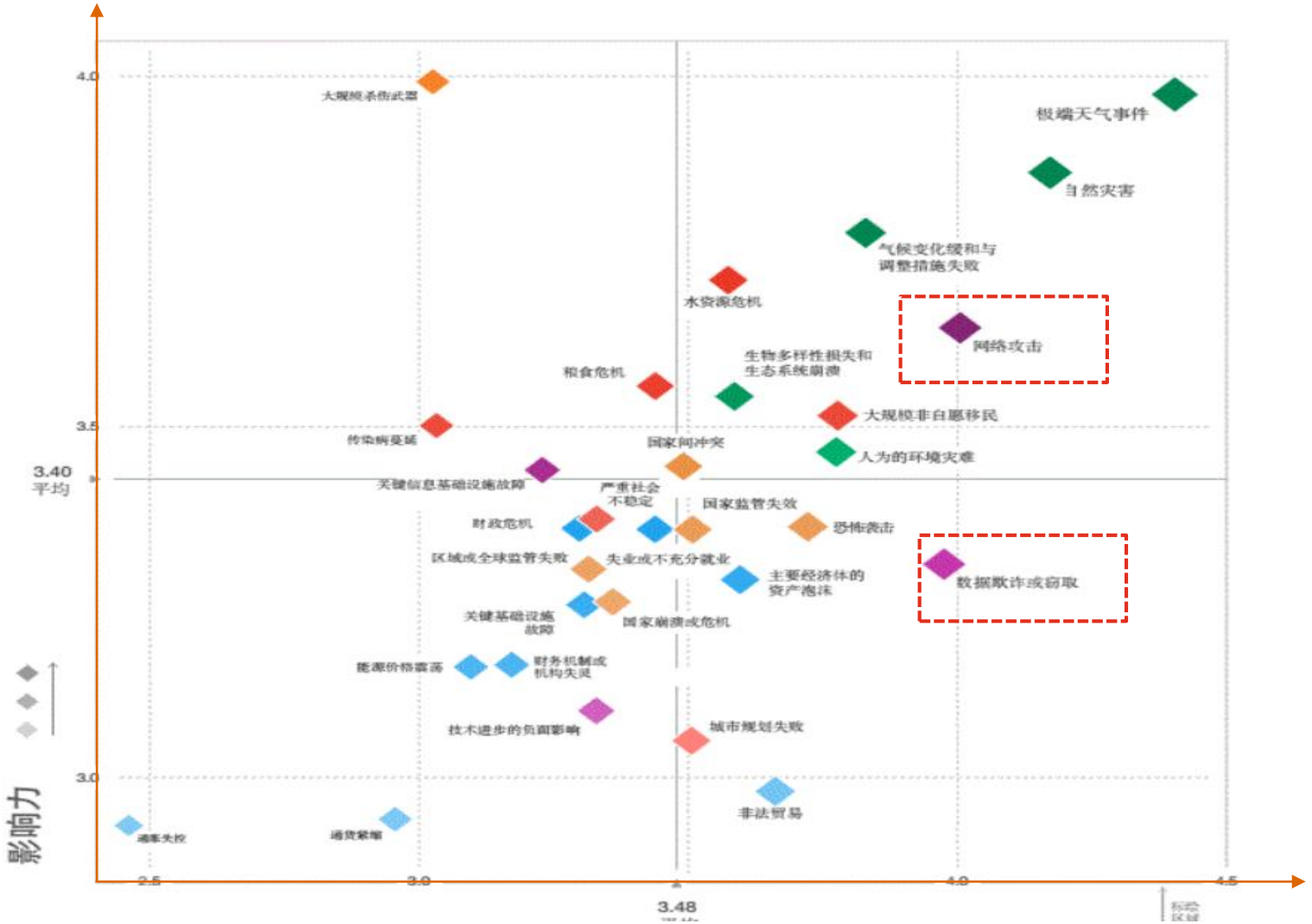
清华经管EMBA 战略课程
TMT 行业导师（2014-2016）



演讲议题

1. 不再安全的世界
2. GDPR的挑战和契机
3. 企业数据安全合规应对之道

最坏的时代—全球网络安全风险进一步升级



世界经济论坛（WEF）统计显示：网络攻击已成为全球第三大威胁

网络攻击问题已经成为全球仅次于极端天气和自然灾害之外全球性的**第三大威胁，数据欺诈和数据盗窃则成为第四大风险。**这是网络攻击首次被列入该组织风险报告前五。

数据来源：世界经济论坛（WEF）发布的《2018年全球风险报告》

最坏的时代--全球数据安全事件频发

1400万 Verizon

2017年7月的ZDNet的一份报道称，有超过1400万Verizon客户的个人数据遭到泄露，这次事件突出了将数据保护实践迁移到云的重要性。
据称，这次安全失误涉及技术提供商Nice Systems，它让Verizon客户数据在AWS S3存储实例上处于未被保护的状态。数据包含姓名、电话号码以及可能被用于访问其Verizon账户的PIN码。
有多达1400万订阅用户受到影响，占到Verizon公司1.8亿总订阅用户的10%。受影响的订阅用户主要是那些在最近6个月中调用了Verizon客户服务的人

5700万 Uber

Uber在2017年11月发现，黑客在去年一次大规模数据泄露事件中窃取了来自5700万名乘客和司机的信息。Uber在2016年10月向盗贼支付了10万美元用于删除数据并对泄露事件保密，据彭博社的报道称。
Uber公司首席执行官Dara Khosrowshani表示，被黑客盗取的乘客和司机信息中包含来自第三方服务器的电话号码、电子邮件地址、以及姓名。而向盗贼支付费用这件事情是前首席安全官Joe Sullivan安全的，后者已经被解雇了。
这次交易是由前CEO Travis Kalanick安排监督的，后者已经在8月离开公司

1.43亿 Equifax

Equifax在2017年9月份透露，一次规模庞大的数据泄露导致其1.43亿信用和信息服务客户受到影响。这些事件最早是在7月29日发现的，是由美国网络应用的一个漏洞导致，该漏洞允许黑客访问某些特定文件。泄露的信息包含姓名、出生日期、社会保障号码、地址和一些驾照号码信息，此外还有20多万个信用卡号码和近20万个其他带有个人身份信息的文件。
就在该泄露事件发生不到三周之后，该公司宣布首席执行官Richard Smith将退休。他的离开立即生效

52GB D&B

世界著名的商业信息服务机构Dun&Bradstreet经历了一起严重的数据泄露事件，一个大小为52GB的数据库意外在线泄露，包括AT&T、沃尔玛、Wells Fargo、美国邮政，甚至美国国防部等在内的3300多万员工的信息和联系方式等。经分析共发现33698126条记录，包含详细的联系方式、职位名称、邮箱地址、电话号码以及雇主信息等。据了解，D&B的全球商业数据库覆盖了超过1亿条企业信息，并通过邓白氏特有的内部流程对每天收集的原始数据进行编辑、核实，以保证数据质量。可见，目前商业网站仍是黑客攻击的主要目标之一

5000万 Facebook

2018年3月16日，Facebook 被曝在2014年有超过5000万名用户（接近Facebook美国活跃用户总数的三分之一，美国选民人数的四分之一）资料遭剑桥分析公司非法用来发送政治广告，部分媒体将其视为 Facebook 有史以来遭遇的最大型数据泄露事件
剑桥分析公司的丑闻对脸书的公司品牌造成了巨大损害。如今要想恢复公众对脸书在隐私保护和数据保护上的信任，需要付出更为巨大的努力。

最坏的时代—个人信息泄露在当下到底有多严重？

1800余起

4个月侦破个人信息相关案件1800余起

500亿条

查获非法倒卖个人信息500亿条，平均每个人被卖30遍

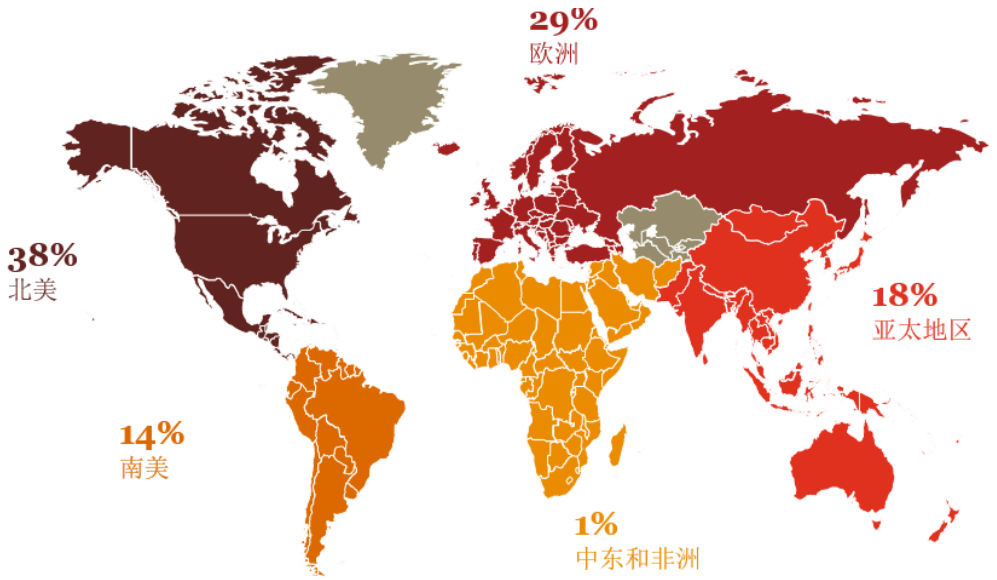
6.88亿人

一年时间国内**6.88亿**网民因受诈骗信息、个人信息泄露等造成影响

0.08元/条

单价低到令人咋舌，1万条隐私数据仅需800元

2018PwC全球信息安全状况调研揭露风险根因



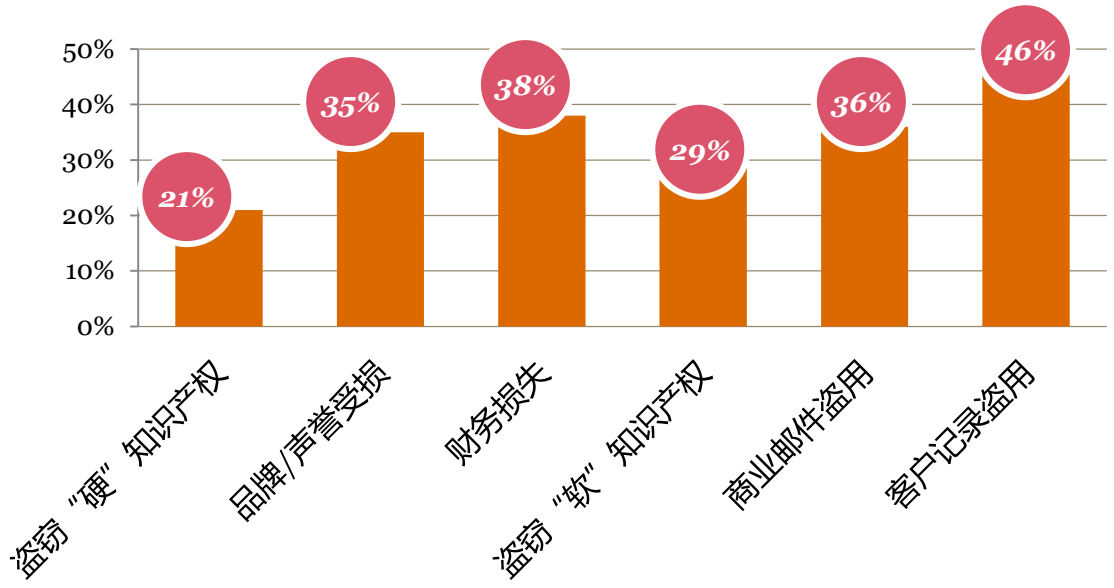
2018全球信息安全状况调查（The Global State of Information Security® Survey 2018），是由普华永道和CIO与CSO杂志联合开展的全球范围调查研究，于2017年4月至5月在互联网上进行

- 普华永道是第***20***次开展这项年度网络调研，也是第15次与*CIO*和CSO杂志合作
- 调研对象来自CIO和CSO杂志的读者与普华永道的客户群体，涵盖***122***个国家
- ***超过9,500***份调研来自CEO（首席执行官）、CFO（首席财务官）、CIO（首席信息官）、 CISO（首席信息安全官）、 CSO（首席安全官）、VP（副总裁）以及IT与安全总监
- ***46%*** 的受访企业年收益超过五亿美元
- ***超过40个***问题涉及信息与隐私保护，企业对先进安全技术的运用
- 从受访者的地域分布来看，*38%*来自北美，*29%*来自欧洲，***18%来自亚太地区***，14%来自南美， 1%来自中东和非洲
- ***中国内地及香港***的受访者超过***460位***

客户数据泄露依然是企业面临的最大挑战，同时网络勒索将会愈发频繁，致使信息系统运行中断，破坏商业机会

最近，通过网络勒索获得企业赎金已经成为黑客惯用的方式，一些能源公司、教育机构、金融机构、旅行社等纷纷中招。此类事件引发的财务损失可能会继续攀升。

安全事件对企业的影响（中国内地/香港）



表示客户记录盗用

中国内地/香港

表示客户记录盗用

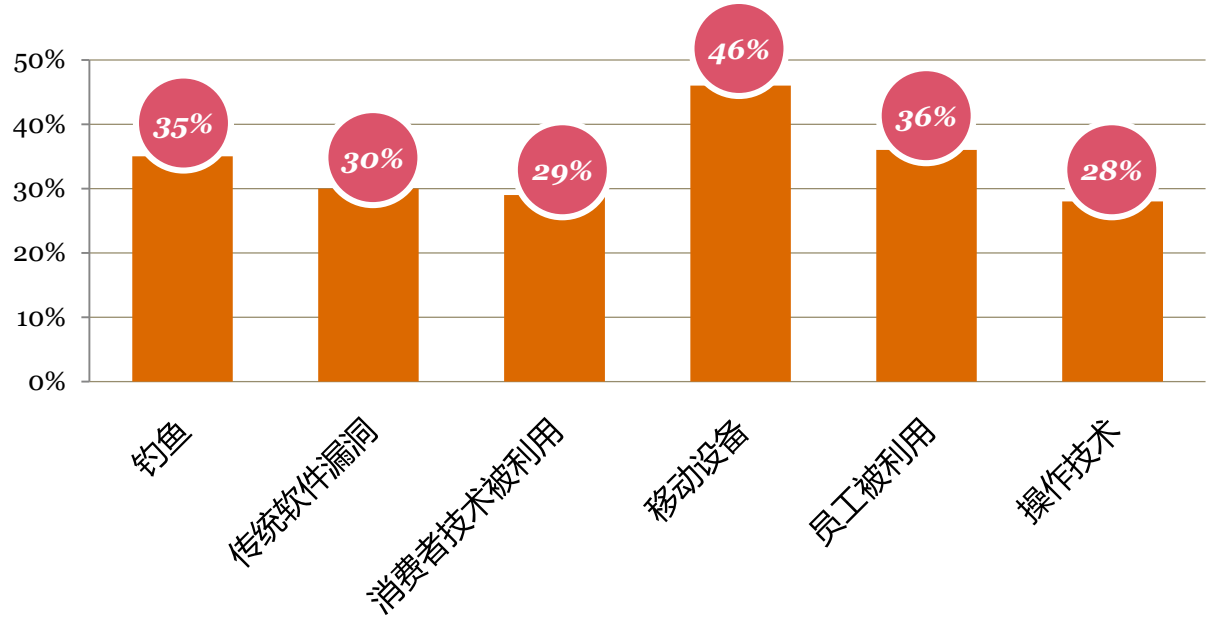
全球

问题22：“你的企业如何受到安全事件的影响？”（并非所有的因素都显示出来）

移动设备成为信息安全事件主要攻击途径

移动设备安全在移动计算中变得越来越重要。随着越来越多的个人和企业使用智能手机或平板电脑进行通信，移动设备成为攻击的首选目标。

企业安全事件的起因（中国内地/香港）



问题19：“安全事件是如何发生的？”（并非所有的因素都显示出来）

将移动设备视为安全事件的原因，比例大过钓鱼手段

中国内地/香港

将移动设备视为安全事件的原因，比例大过钓鱼手段

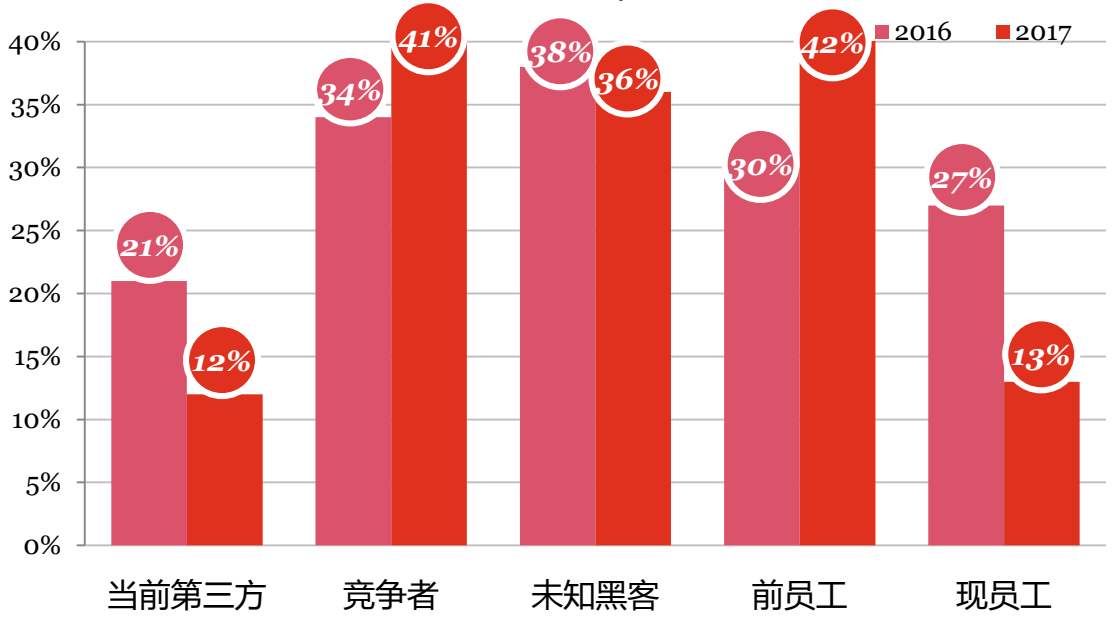
全球

前雇员是安全事件的头号来源

黑客、现有第三方和现有员工引发的安全事件有所下降，而竞争对手（中国内地/香港 41%vs Global 20%）和前员工（中国内地/香港 42%VS Global 26%）的比例则上升。

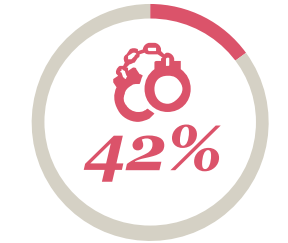
此外，42%的中国内地与香港受访企业认为前雇员是导致安全事件发生的重要来源，这一比例要远高于全球其他国家和地区。

引发安全事件的源头（中国内地/香港）



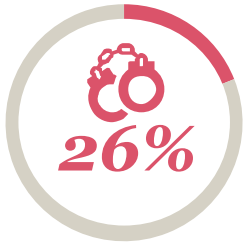
*目前的第三方包括供应商，顾问和承包商

问题21：“事件的可能来源”（并非所有因素都显示）



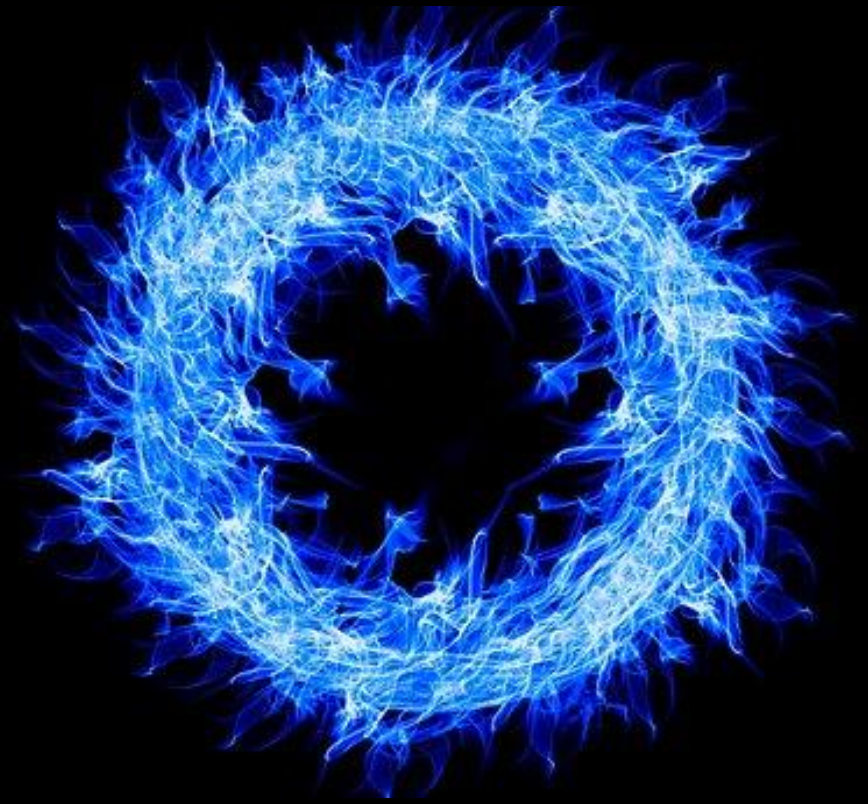
事件是由于前雇员导致的

中国内地/香港



事件是由于前雇员导致的

全球



演讲议题

1. 不再安全的世界
2. GDPR的挑战和契机
3. 企业数据安全合规应对之道

GDPR内容简介 —— 11个章节、99项条款

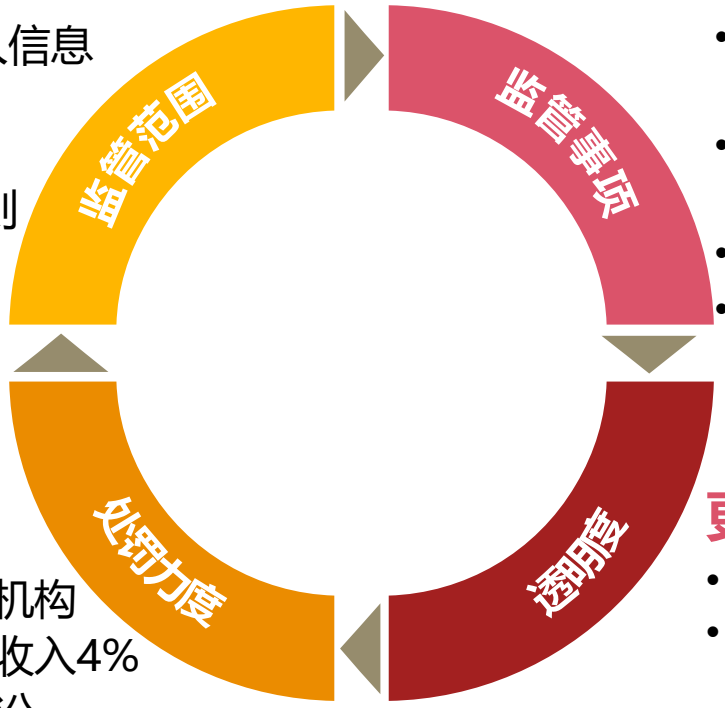
GDPR章节 (共99个条款)
一、一般规定
二、原则
三、数据主体权利
四、控制者和处理者
五、数据出境
六、独立监管机构
七、合作与一致性
八、权利、责任与罚则
九、特定处理情况
十、实施细则
十一、终章

更大的监管范围

- 监管范围更广(个人信息及特殊个人信息)
- 新增隐私保护要求
- 新增隐私保护7原则

更多的监管事项

- 研发过程隐私保护要求(Privacy by Design)
- 隐私影响分析(Privacy Impact Analysis)
- 被遗忘权和可转移权
- 隐私保护专员(DPO)



更严格的处罚

- 授权各国数据保护机构
- 最大罚款上限达年收入4%
- 侵权赔偿及集体诉讼

更广的透明度要求

- 明示同意
- 保护者两种不同角色及对应责任(Controller/Processor)
- 隐私政策公开
- 泄露事件72小时报告监管

GDPR内容简介 —— 11个章节、99项条款（续）

2018年 5月25日 正式生效

GDPR聚焦的核心议题在于数据主体的各项权利，规则中对于数据及相关处理技术的使用加大了关注。

基于GDPR：

- 更多的企业实体将会被监管，其中包括单纯的数据处理方及非欧盟企业实体在内
- 合规的要求将会被扩展到隐私影响评估、默认隐私设计、被遗忘权、数据可移植保护等方面
- 更加严格的透明机制要求了清晰的授权同意书及信息泄露的通报
- 随着扩大监管力而增加的法律法规风险，例如：高额的罚金、集体诉讼及赔偿要求等

GDPR的关键要素:

被遗忘权: 客户有权要求组织删除其原始目的不再需要的个人资料

数据可移植保证: 客户有权因为变更公司而要求将他们的个人资料从一个组织转移到另一个组织，组织机构有义务帮助实现该要求

透明机制: 公司对于处理个人数据的授权同意书需清晰明确

数据泄露通报: 公司将仅有72小时向监管机构披露个人信息方面的泄露，在某些情况下会同时向受影响的个人披露

数据存储: 客户及监管机构有权了解所有数据存储位置

默认隐私设计: 组织机构将被要求尽可能减少收集和使用个人数据，并且在设计新产品和服务时，自动遵循此要求

数据保护责任: GDPR强制要求按一定标准雇用数据保护员（DPO）

你是否了解

- 可高达**全球年营业额4%**的罚款
- **用户行为**的直接权利
- **72小时内**报告信息泄露
- 适用于**非欧盟企业实体**
- 对于数据的定义拓展为:
  - 原始数据
  - IP地址
  - RFID标签
  - Cookie缓存
  - 虚拟匿名化数据

GDPR要点 —— PII 和 SPII

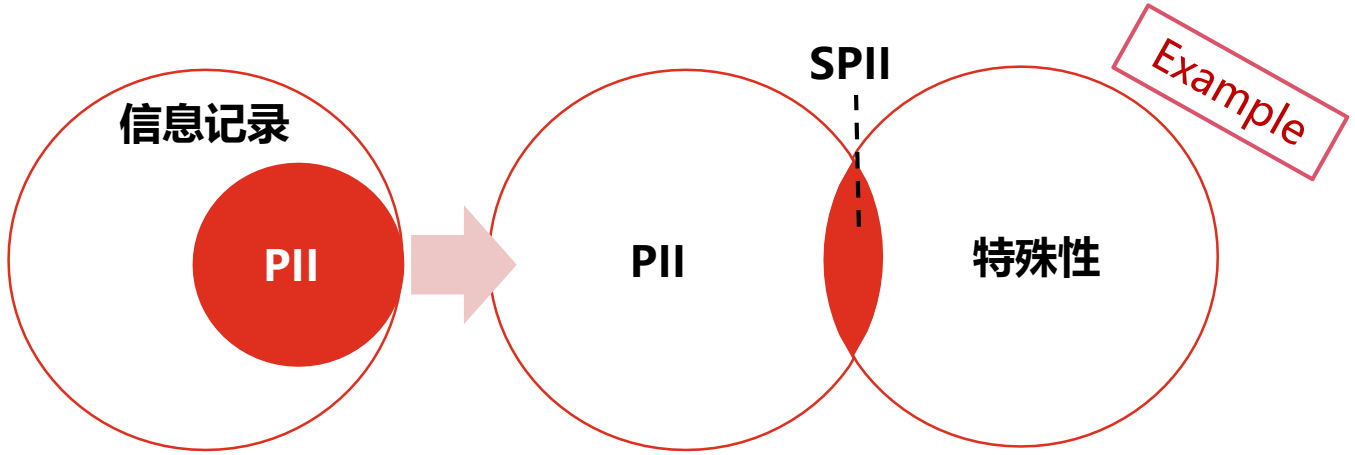
GDPR中规范了“个人数据 - PII”及“特殊个人数据 - SPII”的定义，PII及SPII信息也是欧盟GDPR中要求的隐私保护实际主体，通常情况下，对于SPII数据需进行更加严格的隐私保护。

明确PII/SPII定义

根据GDPR中的要求，“个人数据 - PII”是指任何指向一个已识别或可识别的自然人（”数据主体”）的信息。

该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如**姓名、身份证号码、定位数据、在线身份**识别这类标识，或者是通过参照针对该自然人一个或多个如**物理、生理、遗传、心理、经济、文化或社会身份的要素**。

“特殊个人数据 - SPII”是指对揭示**种族或民族出身，政治观点、宗教或哲学信仰，工会成员**的个人数据，以及以唯一识别自然人为目的的**基因数据、生物特征数据、性生活或性取向**的数据。



PII及SPII示例

以某新兴互联网公司为例：

PII数据：手机号、住址、身份证号、银行卡号、定位数据、MAC、IP地址等；

SPII数据：个人指纹、面部特征、政治及宗教信仰等。

GDPR要点 —— Controller 和 Processer

角色定义

数据控制者（ Controller ）

指**单独或者与他人共同确定个人数据处理的目的、条件和手段**的自然人、法人、公共机构、政府部门或其他机构。

如针对用户在企业电商平台、网站的注册信息，企业是数据控制者。

数据处理者（ Processor ）

指**代表数据控制者处理个人数据**的自然人、法人、公共机构、政府部门或其他机构。

如企业针对企业客户提供服务、提供产品所协助处理或者存储的数据，是数据处理者。

原则	适用的角色	
	数据控制者	数据处理者
正当、合法、透明	√	N/A
目的限制	√	N/A
数据最小化	√	N/A
准确性	√	N/A
存储最小化	√	N/A
完整性与保密性	√	√
可归责	√	√

GDPR要点 —— 数据跨境

场景

如果在欧盟内部，个人隐私数据是否可以自由传送？如果个人隐私数据需要跨境，比如去送去美国、日本、中国、印度等国家进行深入分析，该如何处理？

GDPR相关条款

Chapter V
Transfers of personal data to third countries or international organisations
A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

解决方案

在欧盟之间可以自由传输，如果传到欧盟之外，需要满足以下一种或几种条件：
1. Adequate level of security
收方所在法域、组织或行业能满足同等级别的安全控制（目前中国不具备）；
2. Binding corporate rules
需欧盟的成员国监管机构批准；
3. Standard data protection clauses
成员国监管机构通过，欧盟委员会批准；或直接由欧盟委员会通过；
4. Approved codes of conduct or approved certification mechanisms
如果只涉及一个成员国，由该成员国监管机构批准，如果涉及多个成员国，最终要欧盟委员会批准。

GDPR要点 —— 用户权利

GDPR中规范了包括访问权、纠正权、清除权、限制处理权、持续控制权、广告拒绝权、自动化识别拒绝权在内的7项用户权利。

用户权利	具体描述	处理时效
访问权	用户有权让数据控制者告知如下信息： 个人数据是否被处理、处理的目的；个人数据的类别；已经或未来将要披露给的个人数据接收者或其分类；个人数据存储预设期间；用户应享有的个人数据纠正、清除、限制处理、拒绝处理的权利；用户向监管机构投诉的权利；个人数据来源（当非从用户处获得信息时）；自动化决策的存在、逻辑、重要性和后果；跨境传输采取（如涉及）的适当安全保障措施。 用户可要求数据副本。	一个月内
纠正权	对不正确不完善的信息进行纠正完善，完成后通知用户。	立即
清除权	在撤回用户同意等情形下，需清除相关数据，并通知数据处理者清除数据。	立即 （适当时间内）
限制处理权	在如需核实不准确信息等情形下，除存储数据以外不进行其他处理，即冻结账户；实施限制处理前通知用户。	一个月内
持续控制权	涉及自动化方式决策处理数据的情况下，保证其结构化、通用化、可机读格式，不阻碍用户将数据转移给其公司。	一个月内
广告拒绝权	用户有权拒绝使用其个人信息进行精准化营销。	一个月内
自动化决策拒绝权	用户有权拒绝用户画像类自动化决策并对其实施影响的功能。	一个月内

GDPR生效，已对国内外多个行业的企业产生巨大影响

越来越多的企业在利用技术来彻底改变企业的运营方式或触角。数据作为数字化转型的根基，对企业来说至关重要。自2018年5月25日，GDPR正式实施以来，已对国内外多个行业的多家企业产生巨大影响

GDPR对各企业产生的影响

罚款或诉讼

37亿欧元

39亿欧元

amazon

面临隐私监管机构的诉讼

服务关停

Los Angeles Times

Chicago Tribune

多家美国媒体网站在欧洲的服务器关停

产品升级

AIR CHINA 中國東方航空 CHINA EASTERN

包括互联网企业、航空企业在内的多家企业对海外版产品进行升级或更新其隐私政策，并要求用户重新授权

合规建设

Haier

HUAWEI

海尔和华为等企业聘请专业的团队来应对GDPR的合规要求

GDPR对中国企业的适用性

分类	关联
新零售（电商）企业	线上向欧盟境内数据主体提供商品及服务
在欧盟境内有分支机构的企业	为欧盟境内数据主体提供商品及服务
数据处理企业	为欧盟境内的数据管理者提供数据处理服务
无欧盟境内业务企业	存储或处理欧盟境内数据主体的个人信息

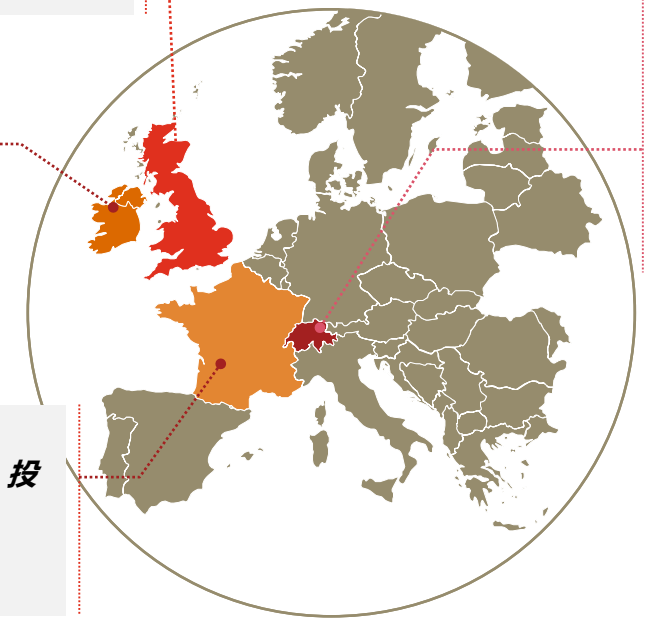
全球多家企业面临针对违反GDPR的诉讼案例

英国
英国信息专员办公室ICO：
3周内收到了1106项数据保护投诉

爱尔兰
官方：收到
403份通知和
89份适用GDPR的投诉

奥地利
官方：已有100多起投诉和59起违规通知

法国
CNIL：与去年同期相比，投诉数量增加了50%



数据来源：Jelinek报告

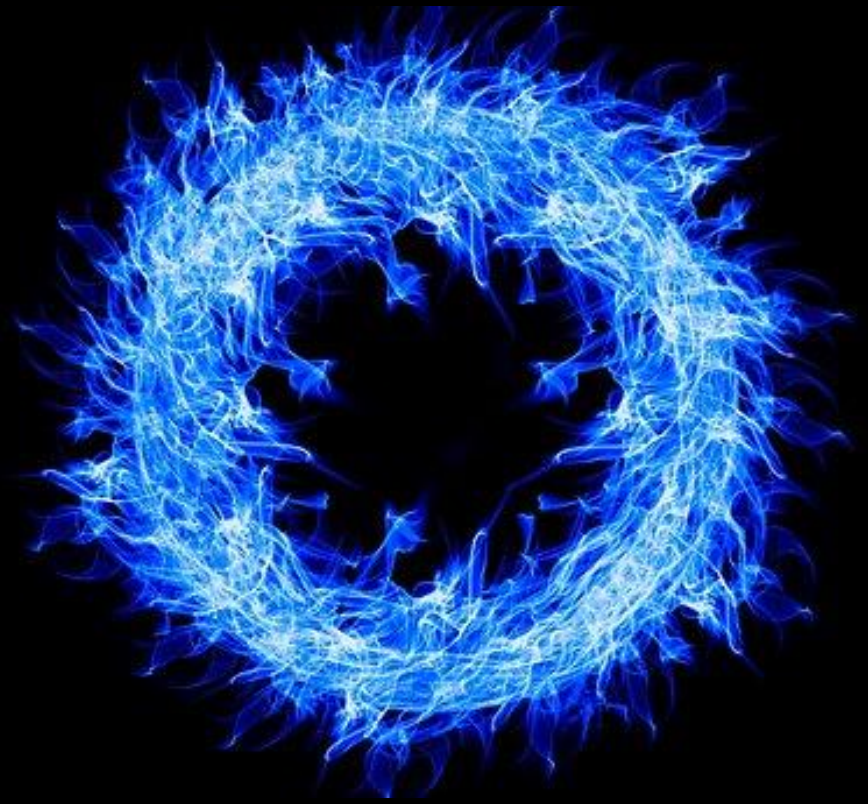
ICANN与Epag全球首例GDPR诉讼案

时间：2018年5月25日

诉讼经过：原告互联网名称与数字地址分配机构ICANN向德国波恩州法院提出了要求法院颁布初步禁令的动议，目的是为了禁止和其签署协议的被告EPAG拒绝根据协议收集域名注册人的个人数据

依据：

- ❑GDPR第5条第1（c）个人数据收集的最小化原则；
- ❑GDPR第25条要求服务和产品按照“隐私默认”和PbD原则设计



演讲议题

1. 不再安全的世界
2. GDPR的挑战和契机
3. 企业数据安全合规应对之道

企业如何确保用户数据的安全直接影响到公共对企业的信任程度

- 公众对企业缺乏信任是企业增长面临的一大威胁
- 数字化和大数据应用使网络安全风险与日俱增
- 妥善管理数据会让企业脱颖而出

图8：数据和信任

问：在数字化程度不断提高的背景下，您在多大程度上同意或不同意以下表述?

以下比例代表表示“同意”或“非常同意”的保险业受访CEO

资料来源：普华永道第20期全球CEO调研

数据来源：普华永道第20期全球CEO调研

企业数据安全关注热点

个人信息防泄漏

- 《中华人民共和国网络安全法》、《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》
- 用户对于个人信息保护意识不断加强

数据安全使用

- 行业数据规模快速扩大、数据类型多样、数据价值增大
- 数据合规性要求趋严，如何合法有效地获取信息，如何保护数据，将成为影响企业声誉和业务经营的关键性因素

综合防御能力

- 随着行业信息化水平的进一步提升，企业对信息系统的依赖性将不断上升，与此同时系统复杂度成倍增长，极可能导致传统的单点防御方式失效

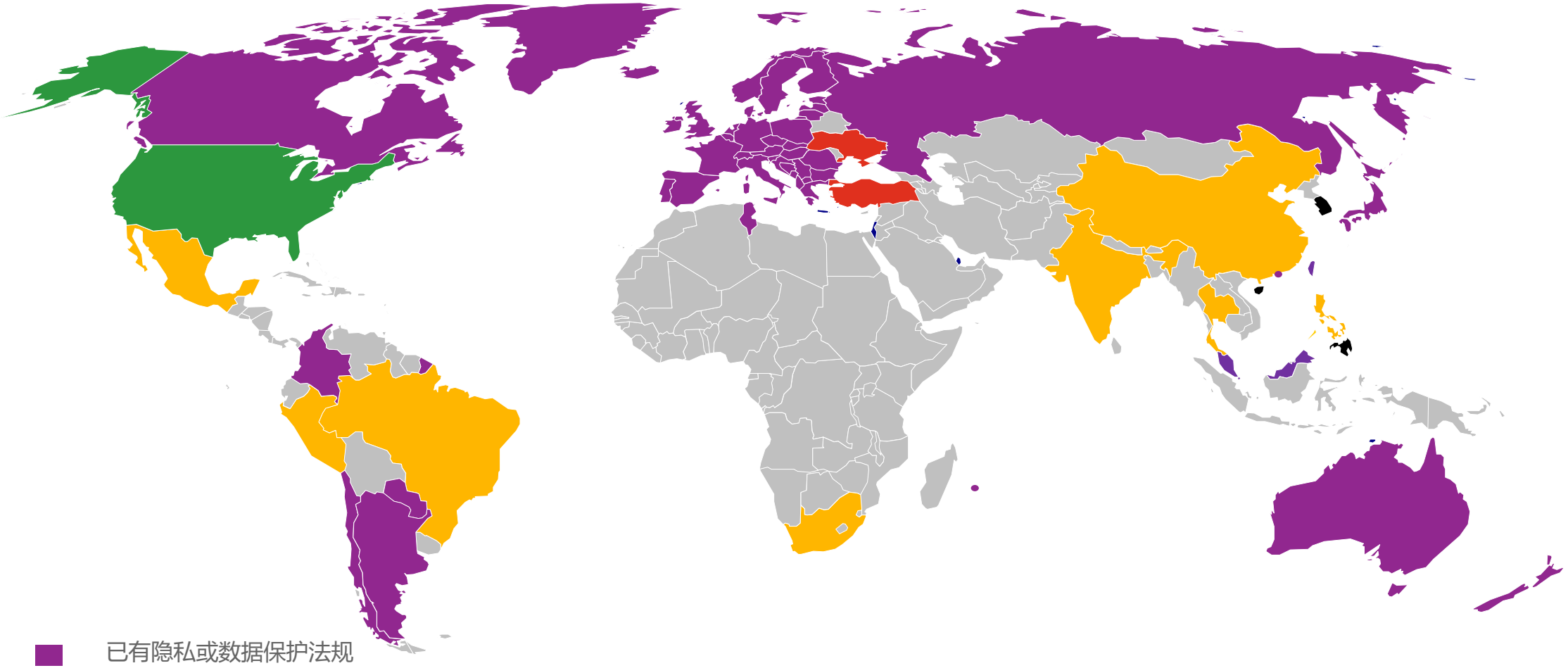
新技术的应用

- 企业对于新兴技术应用的热情（尤其是国内企业对新兴技术的应用十分乐观），可能导致存在安全隐患的技术仓促实施

外部相关方的管理

- 随着业务的拓展，会有越来越多的合伙和外包行为，引入大量的外部相关方参与到业务当中，而外部相关方的安全能力将直接影响到企业的安全能力

全球个人隐私保护概览



结语

“墨菲定律”

1. 会出错的事总会出错;

2. 如果你担心某种情况发生，那么它就更有可能发生;

3. 任何事都没有表面看起来那么简单;

4. 所有的事都会比你预计的时间长.

.