

2017

政企机构信息泄露形势分析报告



360威胁情报中心

2017 年 12 月 12 日

摘 要

- ✧ 信息泄露，是政企机构面临的重要安全风险之一。2017 年以来，国内外均有大量重大的信息泄露事件被媒体曝光，泄露信息少则数十万条，多则数亿条，信息泄露的危害也引起了整个社会的高度关注。信息泄露已经成为安全风险问题的风险源头。

网站漏洞泄露信息风险分析

- ✧ 2017 年 1 月至 10 月，补天平台共收录可导致信息泄露的网站漏洞 251 个，较 2016 年的 359 个下降了 30.1%，约占补天平台全年漏洞收录总数（16427 个）的 1.5%，涉及网站 150 个，共可能泄露信息 51.2 亿条。
- ✧ 从危险等级看，高危漏洞数量占 97.6%，中危占比为 2.4%。
- ✧ 从漏洞的技术类型看，命令执行（占比为 63.7%）、代码执行（14.7%）和 SQL 注入（8.8%）占比最高，三者之和占全部信息泄露漏洞的八成以上。
- ✧ 在 251 个可导致信息泄露的网站漏洞中，共有 24 个网站漏洞可能泄露的信息在 5000 万条以上，其中还有 11 个漏洞可能泄露的信息数量在 1 亿条以上。
- ✧ 补天平台收录的信息泄露相关漏洞中，有 85.3% 的相关漏洞泄露的属于个人信息，14.7% 相关漏洞泄露的属于机构机密信息。
- ✧ 在 251 个可能泄露信息的网站漏洞中：约 85.7% 的网站漏洞可能泄露用户的实名信息，可能泄露实名信息数量多达 42.9 亿条；约 14.7% 的网站漏洞可能泄露机构机密信息，可能泄露机构机密信息数量多达 5.6 亿条。
- ✧ 在 251 个补天平台收录的信息泄露漏洞中，备案的网站漏洞有为 236 个，占比 94.0%。在已备案的网站中，被报漏洞的企业网站数量是最多的，占比为 74.2%。
- ✧ 从可泄露的信息数量来看，不同备案类型网站漏洞可能泄露信息数量的差异较大。企业网站漏洞可能泄露的信息数量最多，分别为 43.9 亿条，约为全年可能泄露信息总量的 85.8%。另外，未备案网站的漏洞可能泄露的信息数量也约占全年泄露总量的 6.9%。
- ✧ 金融网站、政府机构及事业单位网站、通信运营商网站被报告的可泄露信息的漏洞最多，占比分别为 28.3%、26.7%、24.7%，三大行业网站的漏洞报告数量约占所有网站被报告漏洞数量的 79.7%。
- ✧ 从可能泄露信息数量来看，金融行业（22.1 亿条）、通信运营商（18.9 亿条）网站可能泄露的信息数量也是最多的，远高于其他行业。

国内、外机构重大信息泄露事件分析

- ✧ 政府及事业单位的重大信息泄露事件：2017 年，国内发生了一系列的政府机构泄露信息事件。让人惊讶的是，这些事件大多是由于政府网站在政务公开环节，不必要的公开了相关人员完整的、详细的身份信息而造成的，被不当公开的信息包括完整的身份证号码，联系电话等信息。
- ✧ 国外军事机构重大信息泄露事件：军事机构的内部信息无疑是最为敏感的机密信息。在

2017 年媒体披露的军事机构重大泄密事件中，美国上榜次数最多。CIA、NSA、美国国防部，美国陆、海、空军等都未能幸免。从国外军事机构机密信息泄露的原因和结果来看，主要有以下几个明显的特点：内鬼问题；供应链安全问题；网络武器成为攻击目标；低级运维错误仍普遍存在。

- ✧ 国外政府机构重大信息泄露事件：2017 年媒体公布的国外政府机构重大信息泄露事件中，美国和印度的上榜次数最多。国外政府机构的信息泄露事件主要表现出以下几个明显特点：政府机构信息泄露的重要原因在于网络服务商或云服务商的管理疏失或安全漏洞；超大规模的信息泄露事件频发，泄露信息数量动辄上千万；政府机构泄露的公民个人信息往往是综合性信息，包括姓名、身份 ID（如身份证号码）、家庭住址、家庭关系、工作情况、电话号码和电子邮箱等。
- ✧ 国外金融行业重大信息泄露事件：国外金融机构的信息泄露事件主要表现为以下几个特点值得关注：信息泄露伴随财产损失；误操作也可能引起重大损失；内鬼问题和技术窃密值得关注。
- ✧ 交通行业重大信息泄露事件：交通行业发生重大信息泄露事件的机构主要集中在民航和汽车领域。泄密原因多种多样，其中也有一些高级机密信息泄露的事件发生，如英国女王安保路线这样高度机密的信息被泄露等。
- ✧ 国外互联网企业重大信息泄露事件：从 2017 年互联网企业重大信息泄露事件来看，主要表现出以下几个特点值得关注：帐号密码仍然是互联网企业信息泄露的主要形式；技术资料泄密事件多发，并可能引发难以估计的损失；互联网企业的安全漏洞或管理疏失，往往会殃及大量使用这些互联网企业服务的企业和个人；物联网服务可能引发的信息泄露成为现实。
- ✧ 医疗卫生机构重大信息泄露事件：医疗卫生行业的信息泄露一般可以分为病患信息泄露和医院信息泄露两个方面。特别让人担忧的是，病患信息属于极其敏感的个人信息，知名人士病患信息的泄露甚至可能引发社会不安。
- ✧ 传媒机构重大信息泄露事件：2017 年国外传媒机构重大信息泄露事件大多与黑客攻击有关，也有个别情况是由于运维不当造成的。媒体机构泄露信息的内容也是多种多样，包括用户信息、商业机密、尚未发布的内容资源。
- ✧ 旅行、酒店及餐饮业的重大信息泄露事件：2017 年，针对旅行社、酒店及餐饮行业的网络攻击也频繁发生。主要有以下几个特点：针对终端刷卡设备，特别是 POS 机的恶意程序攻击，已经成为一种盗取信用卡信息、进而盗刷用户信用卡的主要手段之一；相关技术手段已经十分成熟；旅行、酒店及餐饮等机构普遍缺乏必要的网络安全管理措施，服务器系统极易遭到入侵和破坏；相比于其他行业机构的信息泄露，旅行、酒店及餐饮行业的信息泄露包括大量的用户生活、出行等隐私信息。

关键词： 补天平台、网站漏洞、信息泄露

目 录

研究背景.....	1
第一章 网站漏洞泄露信息风险分析	2
一、 网站漏洞可泄露信息形势综述	2
二、 网站漏洞可泄露信息类型分析	5
三、 可泄露信息网站的行业分析	6
四、 网站信息泄露的原因与趋势	8
第二章 国内机构重大信息泄露事件分析	9
一、 政府及事业单位的重大信息泄露事件	9
二、 互联网企业重大信息泄露事件	10
三、 医疗卫生系统重大信息泄露事件.....	11
第三章 国外机构重大信息泄露事件分析	12
一、 国外军事机构重大信息泄露事件.....	12
二、 国外政府机构重大信息泄露事件.....	14
三、 国外金融行业重大信息泄露事件.....	16
四、 交通行业重大信息泄露事件	18
五、 国外互联网企业重大信息泄露事件.....	19
六、 医疗卫生机构重大信息泄露事件.....	22
七、 教育机构重大信息泄露时间	22
八、 传媒机构重大信息泄露事件	23
九、 旅行、酒店及餐饮业的重大信息泄露事件	24
十、 其他重大信息泄露事件.....	25
第四章 关于信息数据保护的政策、法规与技术	27
一、 中国《网络安全法》规范数据保护，并对信息泄露事件追责	27
二、 国外政府对信息泄露事件处置的新法规	27
三、 快递行业对于隐私面单的探索实践.....	28

研究背景

信息泄露，是政企机构面临的重要安全风险之一。2017 年以来，国内外均有大量重大的信息泄露事件被媒体曝光，泄露信息少则数十万条，多则数亿条，信息泄露的危害也引起了整个社会的高度关注。信息泄露已经成为安全风险的风险源头。

造成机构信息泄露的主要原因有两类，一是黑客入侵、二是内鬼出卖。而从机构泄露的信息类型来看，主要也分为两类，个人信息和机密信息，后者是指政企机构内部除个人信息之外的商业机密、技术机密及其他机密信息。

在大数据产业迅猛发展的浪潮中，我国个人信息安全和隐私保护面临着严峻形势。个人信息作为数据信息的核心内容，面临着采集、存储、加工、各环节的使用规范化问题，与个人隐私息息相关。目前，一些行业个人信息泄露事件频发，不法分子甚至还会利用已经泄露的海量数据信息进行关联分析，甚至做出客户画像，精准定位用户身份后，实施精准诈骗。

其他类型的机密信息泄露事件也十分让人担忧。例如，微软 1.2GB 的部分 Windows 10 源代码泄露事件，不仅仅会使微软公司本身面临巨大的商业损失，同时也会使 Windows 用户面临更大的安全风险，因为攻击者完全有可能通过泄露出来的源代码，发现 Windows 更多的安全漏洞，并对这些漏洞进行恶意利用。

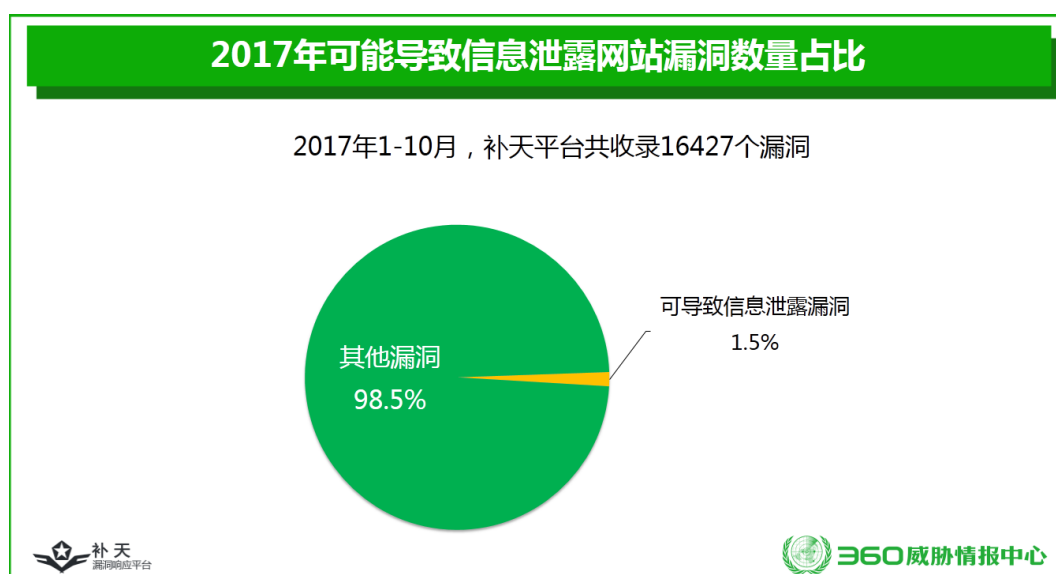
为了更加全面的分析 2017 年以来，国内外政企机构的信息泄露安全风险及由此引发的其他安全问题，本报告将从网站的信息泄露风险，及国内外重大信息泄露事件这两个方面，来系统性的分析政企机构信息泄露的风险及形势。

第一章 网站漏洞泄露信息风险分析

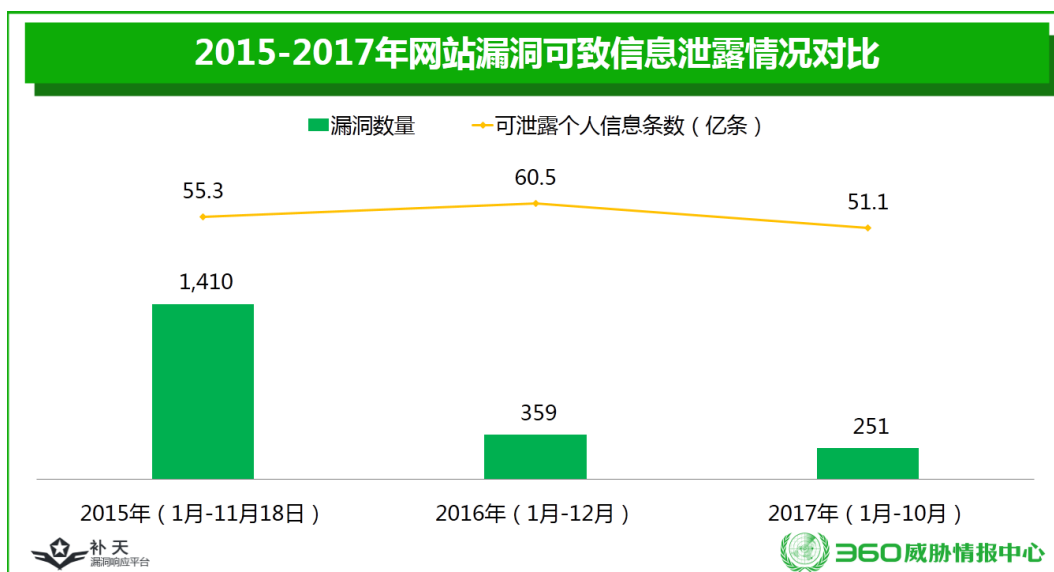
由于网站存在安全漏洞所导致信息泄露，政企机构信息泄露的主要原因之一。本章将主要以补天平台 2017 年 1 月至 10 月收录的可导致信息泄露的漏洞为基础，对 2017 年网站泄露信息的严峻形势进行综合分析。

一、 网站漏洞可泄露信息形势综述

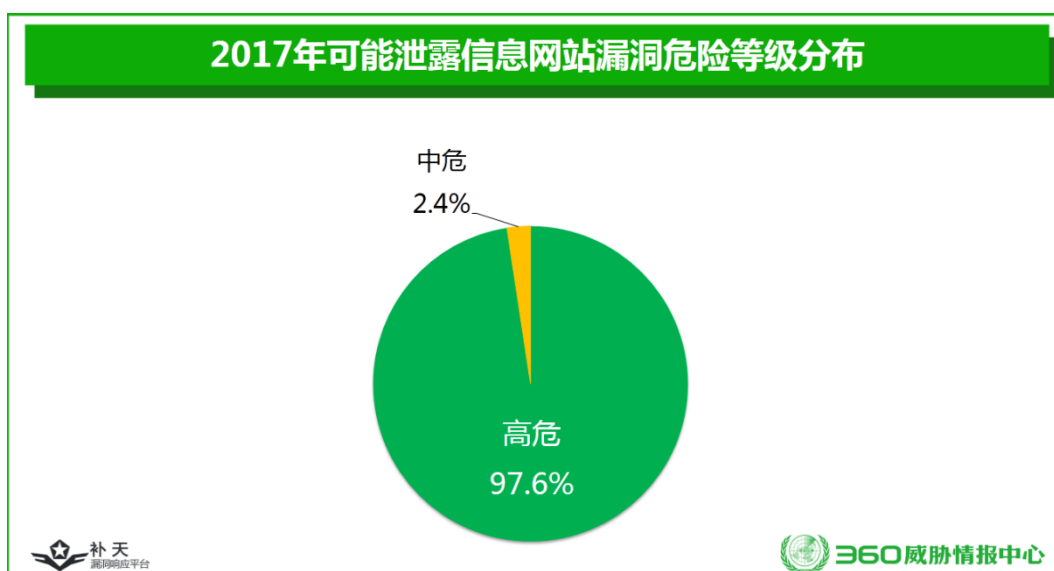
2017 年 1 月至 10 月，补天平台共收录可导致信息泄露的网站漏洞 251 个，较 2016 年的 359 个下降了 30.1%，约占补天平台全年漏洞收录总数（16427 个）的 1.5%，涉及网站 150 个，共可能泄露信息 51.2 亿条。



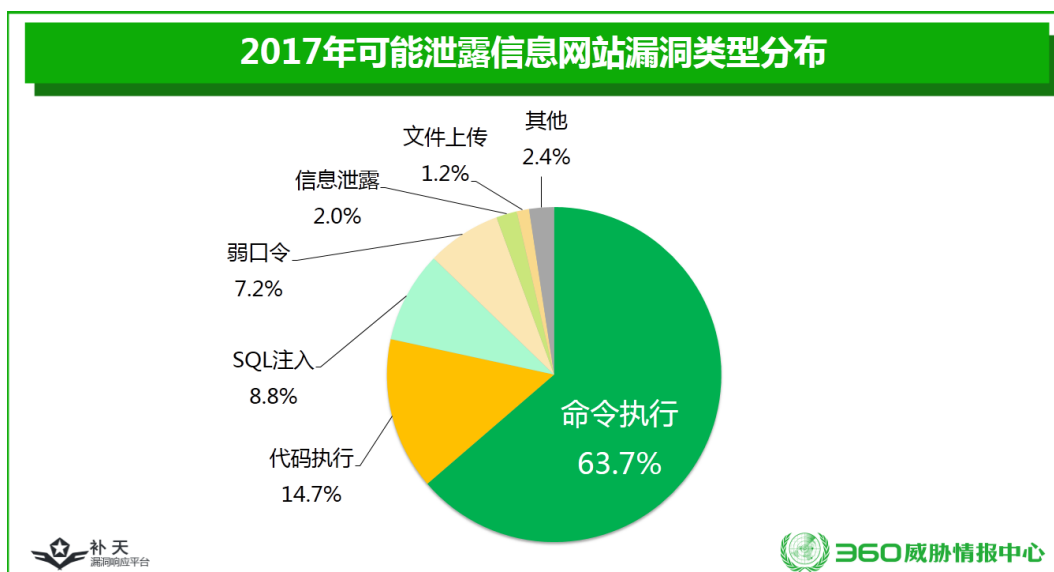
统计显示，251 个可导致信息泄露的网站漏洞，总计可能泄露信息为 51.1 亿条，比 2016 年的 60.5 亿条下降了 15.5%；比 2015 年的 55.3 亿条下降了 7.6%。平均每个漏洞可导致 2035.9 万条个人信息泄露，单个漏洞的危害大大增加。



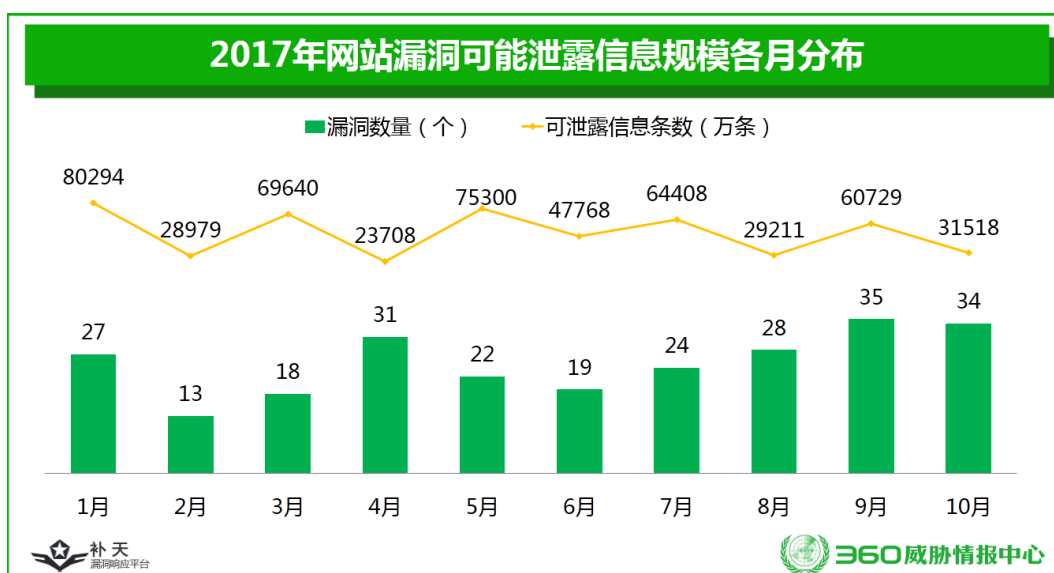
从危险等级看，2017 年可能泄露信息的漏洞中，高危漏洞数量占 97.6%，中危占比为 2.4%。与高危漏洞相比，中危和低危漏洞的利用难度相对较小。



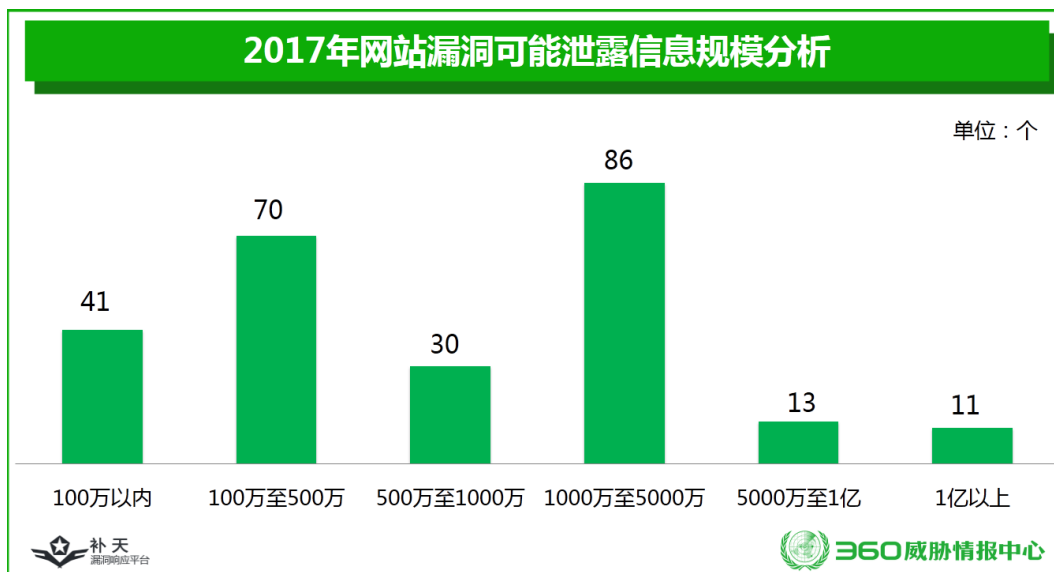
从漏洞的技术类型看，2017 年可能泄露信息的漏洞中，命令执行（占比为 63.7%）、代码执行（14.7%）和 SQL 注入（8.8%）占比最高，三者之和占全部信息泄露漏洞的八成以上。下图给出了相关漏洞的技术类型详细分布情况。



2017年1至10月，补天平台收录的可导致信息泄露的网站漏洞，具体分布情况如下图5个，1月份曝出的可能泄露的信息数量达到最高峰，为8.0亿条信息。

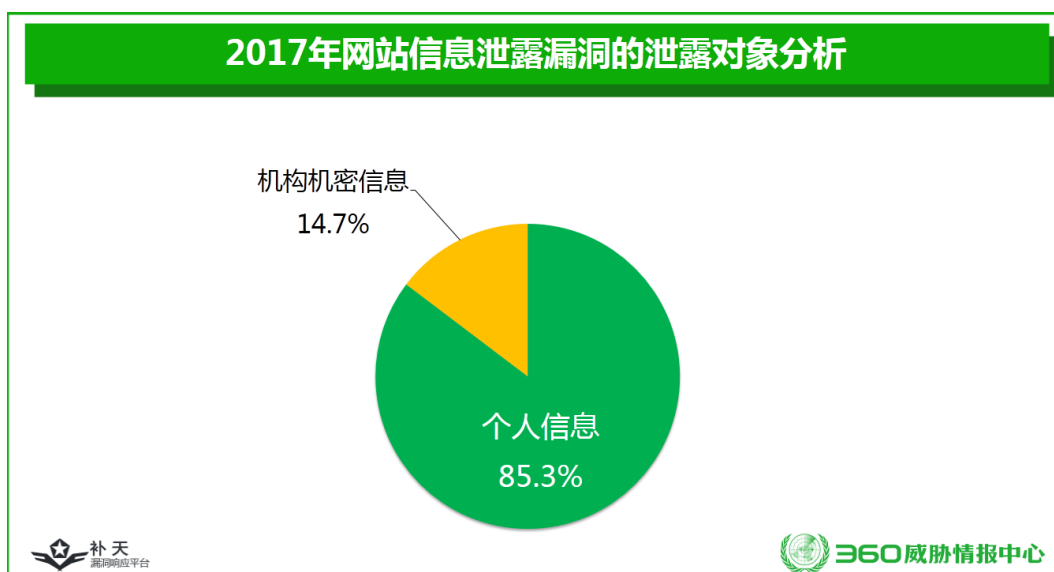


统计显示，在251个可导致信息泄露的网站漏洞中，共有24个网站漏洞可能泄露的信息在5000万条以上，其中还有11个漏洞可能泄露的信息数量在1亿条以上。下图给出了2017年网站漏洞可能泄露信息的规模分析。



二、网站漏洞可泄露信息类型分析

360 威胁情报中心的监测显示，补天平台收录的信息泄露相关漏洞中，有 85.3% 的相关漏洞泄露的属于个人信息，14.7% 相关漏洞泄露的属于机构机密信息。



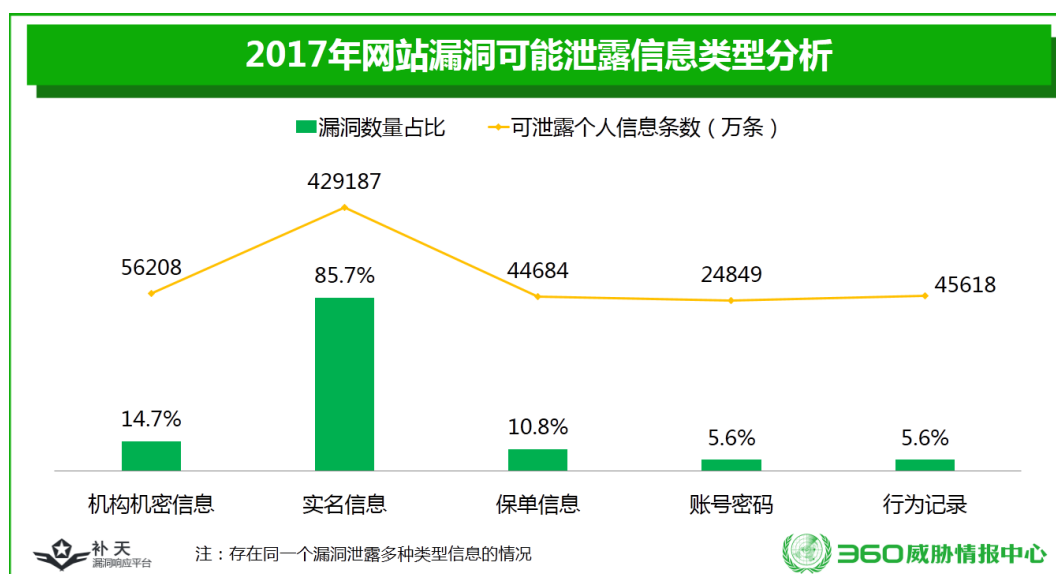
按照数据的敏感度，本报告将补天平台收录的漏洞可能泄露的个人信息数据划分为四个基本类型：

- 1) 实名信息：如姓名、电话、身份证、银行卡、家庭住址等信息。
- 2) 保单信息：保单号、保险信息、车险信息等。
- 3) 帐号密码：如各类网站登录帐号密码、游戏帐号密码、电子邮箱帐号密码等。
- 4) 行为记录：如聊天记录、购物记录、差旅信息等。

而相关漏洞可能泄露的机构机密信息中，根据潜在风险程度，依次主要包括以下几个大类：

- 1) 财务信息
- 2) 合同信息
- 3) 企业资产
- 4) 公司注册信息

统计显示，在 251 个可能泄露信息的网站漏洞中：约 85.7% 的网站漏洞可能泄露用户的实名信息，可能泄露实名信息数量多达 42.9 亿条；约 10.8% 的网站漏洞可能泄露用户的保单信息，可能泄露保单信息数量多达 4.5 亿条；约 14.7% 的网站漏洞可能泄露机构机密信息，可能泄露机构机密信息数量多达 5.6 亿条，具体如下图所示。



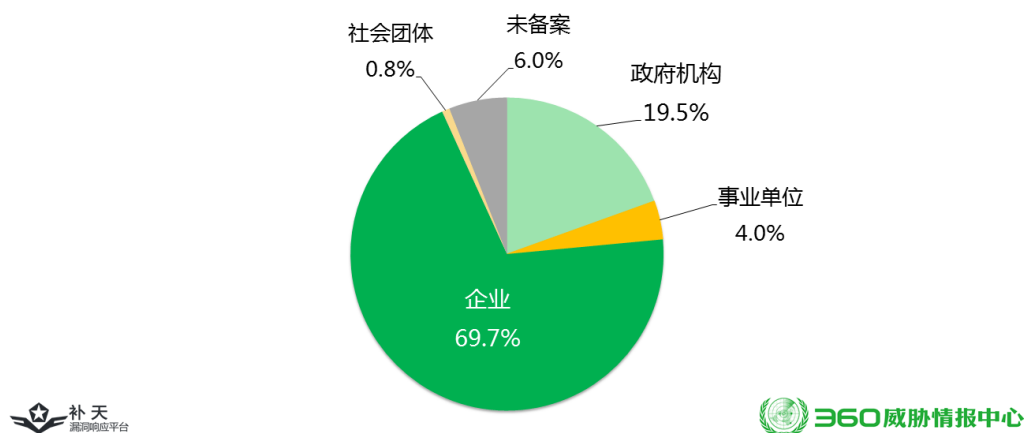
需要特别说明的是，由于网站数据形式的多样性，一个网站漏洞可能泄露的信息的类型未必是单一的，约有 1.6% 漏洞会同时泄露上述 3 种不同类型的信息，约 10.4% 的漏洞会同时泄露上述两种不同类型的信息。

三、可泄露信息网站的行业分析

根据工信部网站查询结果，一般网站备案的类型分为：军队、政府机构、事业单位、社会团体、企业、个人等类型。在 251 个补天平台收录的信息泄露漏洞中，其中有备案的网站漏洞有为 236 个，占比 94.0%。

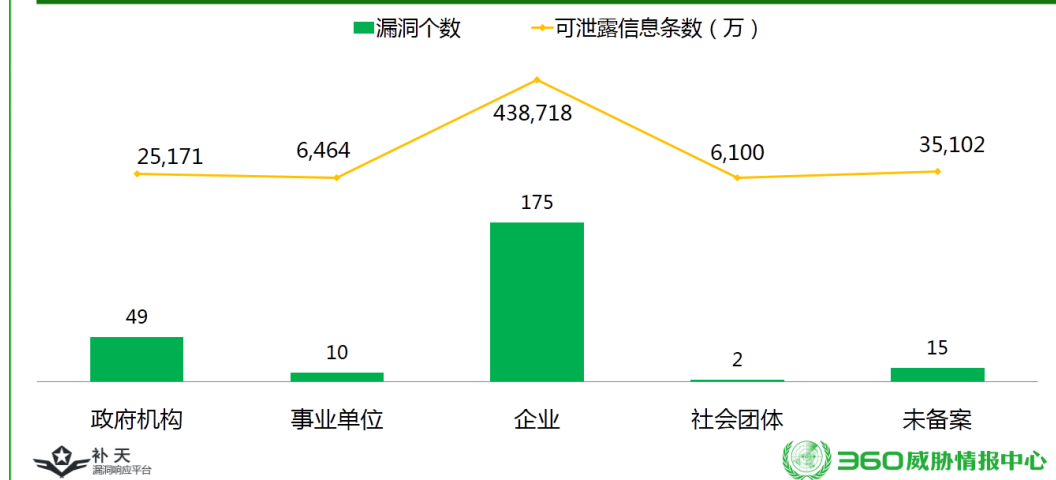
在已备案的网站中，被报漏洞的企业网站数量是最多的，占比为 69.7%，其次为政府机构网站，占比为 19.5%，事业单位网站占比为 4.0%。从下图可以看出，企业和政府机构网站存在的信息泄露漏洞的情况明显多于其他。

2017年可能泄露信息漏洞的网站备案情况分析



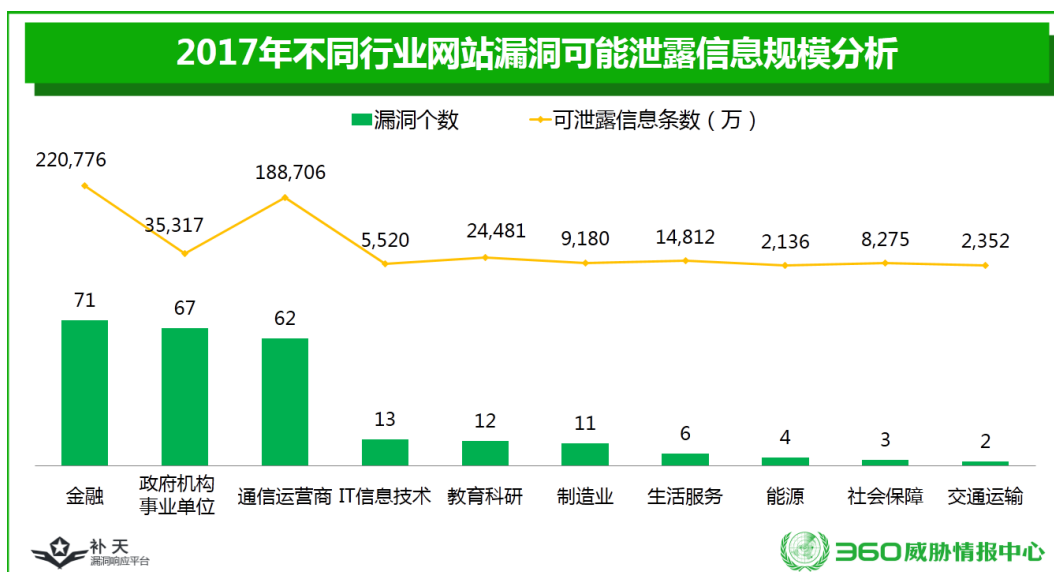
从可泄露的信息数量来看，不同备案类型网站漏洞可能泄露信息数量的差异较大。从下图可以看出，企业网站漏洞可能泄露的信息数量最多，约为 43.9 亿条，约为全年可能泄露信息总量的 85.8%。另外，未备案网站的漏洞可能泄露的信息数量也约占全年泄露总量的 6.9%。

2017年不同备案网站漏洞可能泄露信息规模分析



统计显示，金融网站（金融行业的相关漏洞主要集中在中小保险机构及中小信贷平台，而银行等大型金融机构的安全性相对较高，问题较少）、政府机构及事业单位网站、通信运营商（含虚拟运营商）网站被报告的可泄露信息的漏洞最多，占比分别为 28.3%、26.7%、24.7%，三大行业网站的漏洞报告数量约占所有网站被报告漏洞数量的 79.7%。

从可能泄露信息数量来看，金融行业（22.1 亿条）、通信运营商（18.9 亿条）网站可能泄露的信息数量也是最多的，远高于其他行业。



四、 网站信息泄露的原因与趋势

综合补天平台过去三年来的监测与分析，一个明显的趋势就是可造成重大信息泄露的漏洞数量每年都在大幅下降，但同时，单个漏洞可能造成的信息泄露数量却在大幅增加。这一方面反应出国内网站在信息保护方面的建设在不断加强，整体形式明显好转；另一方面也反应出，信息泄露的风险正在逐步向少数领域集中，而且大型民用服务系统一旦出现安全问题，往往会给整个社会带来巨大的损失。

实际上，信息泄露问题是政企机构数字化转型过程中普遍存在的安全问题。数字化转型较早，信息系统网络化程度相对较高的行业和领域，被暴露出来的问题也相对较多。如金融、通信、新兴互联网等领域。但随着数字化转型的逐渐深入以及网络安全建设水平的不断提高，这些行业或领域在度过信息泄露的高峰期后，安全问题会逐渐缓和。但某些数字化转型相对较晚的行业或领域，如某些大型政府机构、制造业，以及某些传统实体经济，现在暴露出来的问题就相对较少，但在未来不可避免的数字化转型过程中，也必然会逐渐暴露出越来越多的安全问题，面临越来越大的信息泄露风险。

从另外一个角度来看，在消费互联网时代，聚集大量个人服务的信息系统，往往容易成为信息泄露的高发点。而在未来，随着智慧城市的建设，产业互联网的出现，传统的实体经济的互联网化，政务云和互联网+的普及，政府机构和实体经济将有可能面临更大的信息泄露风险，成为信息泄露新的高发领域。

第二章 国内机构重大信息泄露事件分析

2017 年，国内外政企机构均发生了大量的重大信息泄露事件。本次报告通过对国内外媒体公开信息整理，对 2017 年以来，国内外的相关事件进行了总结和简要分析，供读者参考。

本章主要介绍 2017 年媒体报道的国内政企机构发生的一些重大信息泄露事件。总体来看，互联网企业被曝出的信息泄露事件最多，影响也最大。其次是政府和事业单位网站。此外，金融、医疗等行业也有相关的信息泄露事件被曝出。

一、政府及事业单位的重大信息泄露事件

（一）问题综述

2017 年，国内发生了一系列的政府机构泄露信息事件。让人惊讶的是，这些事件大多是由于政府网站在政务公开环节，不必要的公开了相关人员完整的、详细的身份信息而造成的，被不当公开的信息包括完整的身份证号码，联系电话等信息。

这些信息泄露事件的发生，主要是由于有关部门的相关负责人缺乏最基本的网络安全常识，缺乏最基本的公民信息保护意识而引发的“完全不必要的”网络安全事件，而与任何网络攻击技术或网站安全漏洞无关。这也不得不让我们对很多中小城市的网络安全建设水平感到担忧。我们有理由认为，类似的事情在全国各地可能非常的普遍，媒体报道出来的相关情况可能也只是冰山一角。

同时，关于政务公开、重大事件公示等必要的行政措施，与公民个人信息保护之间可能存在的矛盾问题也值得我们进行更深入的思考。表面上看，我们似乎总是可以找到一个平衡点来平衡公开公平与隐私保护之间的关系。但实际上，此类问题涉及法律法规、技术手段、公众认知、公职人员办事能力等多方面的复杂因素，很难在短时间内得到全面有效的解决。

（二）安徽江西等地部分政府网站泄露公民隐私信息

2017 年 8 月，铜陵市铜官区阳光社区服务中心，在铜陵市政府信息公开网发布了《阳光社区 2017 孕前优生健康检查人员名单》。该名单公布了 40 对夫妻的姓名及检查日期，其中 77 人的身份证号码完整呈现，名单仅对现居住地地址做了模糊处理。而在铜官区翠湖社区发布的《2017 年孕前优生检查参检人员名单》中，也完整披露了 23 对夫妻的姓名及检查日期。

2017 年 10 月 10 日，江西省宜春市财政局在宜春市政府信息公开网（xxgk.ycf.gov.cn）发布的《关于公布 2017 年会计专业技术初级资格无纸化考试宜春考区合格人员名单的通知》，也公布了相关人员详细的个人身份证号码的人员名单，910 名合格考生的证书编号、准考证号、身份证号码、姓名等信息予以公开。

2017 年 10 月 31 日，江西省景德镇市政府信息公开网（xxgk.jdz.gov.cn）曾发布了《第二批大学生一次性创业补贴公示》。其中，可供公众下载的文件公布了学生姓名、完整身份证号以及联系电话等。此外，景德镇市人社局官网也可获取上述公示信息。

（三）重庆九龙坡区教委官网泄露上千老教师个人信息

2017 年 11 月，据澎湃新闻报道，重庆市九龙坡区教育委员会官方网站同样存在多份文件泄露教师、学生个人信息的情况，当地相关部门迅速进行了整改。

九龙坡区学生资助管理中心 2015 年 8 月 21 日在九龙坡区教委官网（<http://www.jlpjw.gov.cn>）发布《九龙坡区 2015 年家庭经济困难大学新生入学资助项目资助学生名单公示》。在该公开文件中，家庭经济困难大学新生的姓名、高中毕业学校、身份证号以及录取院校等信息均被公布，共计 65 人。

九龙坡区教委人事科 2016 年 7 月 4 日在九龙坡区教委官网发布了《重庆市九龙坡区教育委员会关于乡村学校从教 30 年教师名单公示》。这份公开文件中，九龙坡区乡村学校从教 30 年、20 年教师的工作单位、姓名、身份证号码、参加工作时间、专业技术职务以及从业状态被完整公布，此外，这份名单人数达 1655 人。

九龙坡区学生资助管理中心 2016 年 8 月 24 日在九龙坡区教委官网发布《九龙坡区 2016 年“金秋圆梦”公益资助大学贫困新生资助学生名单公示》。在该文件中，5 名大学贫困新生的姓名、开卡银行、银行卡号、联系电话等个人信息被公布。

九龙坡区学生资助管理中心 2016 年 9 月 27 日在九龙坡区教委官网发布的《关于 2016 年中央专项彩票公益金教育助学项目资助的公示》中，被资助学生的学校、本人姓名、身份证号码被公布，共计 130 人。

（四）石家庄政府官网大面积泄露执法人员隐私信息

2017 年 11 月，澎湃新闻记者查询石家庄市人民政府官方网站（www.sjz.gov.cn）“信息公开”一栏“石家庄市行政执法监督信息平台”网页发现，该页面中行政执法公示内容涉及到石家庄下辖 22 个县市区政府公开的行政执法人员清单，其中，至少有桥西区、新华区、长安区、井陉矿区、正定县、平山县、无极县等 16 个县市区政府官网中泄露了多个部门行政执法人员的完整身份证号码和手机号码。

同样，在石家庄市桥西区人民政府官方网站“石家庄桥西区行政执法公示专栏”内，财政局、质监局和人社局在行政执法人员清单中完整公布了行政执法人员的姓名、单位、职务、单位性质、身份证号码和执法证号等信息。该区人防办除了公开了行政执法人员完整的身份证号码外，还公布了行政执法人员的个人手机号码，文体局则公布了行政执法人员的姓名、部门职务及个人手机号码。

二、 互联网企业重大信息泄露事件

（一）58 同城数据遭遇爬虫软件

2017 年 3 月，多家新闻网站曝出“58 同城陷数据泄露：700 元可采集网站全部简历信息”的新闻。相关报道指出，在淘宝等电商平台上，有人公开出售一些特殊的爬虫软件，这些爬虫软件可以自动抓取 58 同城网站上的简历数据、本地商户信息、汽车过户信息、保洁公司信息、租房联系人信息等多类信息。自 2016 年初开始，关于 58 同城的爬虫软件和相关技术讨论不断涌现，利用这些工具，一天可采集到的数据量可达 10 万条。

CNNVD（中国国家信息安全漏洞库）发布的关于 58 同城简历泄露事件的通报指出：由于 58 同城网站存在弱加密等设计缺欠，导致攻击者可通过访问该网站的某些数据查询接口，

经过简单的解密还原，获取并关联用户关键信息，进而获取用户简历的全部信息。

这起事件的最可怕之处还不在于有多少个人信息被泄露，而在于可被用于非法窃取个人信息的黑客工具在互联网上被公开销售，这充分的说明了网络黑产交易活动的猖獗，也必将给更多网站和个人带来更大的安全威胁。

（二）优酷上亿条数据千元售卖

2017 年 4 月，黑客“CosmicDark”在网上售卖从优酷窃取约的 1 亿用户账号，售价约 2000 人民币。CosmicDark 称，该数据库于 2016 年被泄，今年才在互联网上公开暴露。但是目前尚不清楚这些数据库是如何被窃取的。

该数据库包含大量帐号的电子邮箱和解密的 MD5、SHA1 哈希密码。CosmicDark 提供的一份样本数据（552 个账号）显示，大多数电子邮箱来自@163.com、@qq.com 和 @xiaonei.com。而且，有黑客资讯网站经过研究发现，样本数据中提供的加密密码已被解密，并公开暴露在互联网上。

用户帐号、密码等信息的盗窃和交易活动一直是网络黑产的主要活动之一。特别是由于很多用户会使用相同的帐号和密码在多个网站上进行注册，常用邮箱也经常被用于各种不同网络应用的注册，所以一旦有某些知名网站或邮箱发生大规模帐号密码泄露事件，就会引发一系列的连锁反应，进而导致更大规模的帐号信息泄露。

（三）50 名小红书用户被骗 88 万

据媒体报道，截至 2017 年 5 月 31 日，先后有 50 名“假冒小红书客服诈骗”的受害者向中国青年报求助，这些受害者因在手机应用“小红书”上网购后遭遇假冒客服而被骗，累计受骗金额高达近 88 万元。据报道，这些用户在小红书上网购之后，都接到自称是“小红书客服”的电话。假冒客服以客户购买的商品存在质量问题而需要退款为由实施诈骗。

据统计，50 名受骗者受骗总金额为 879163.58 元，受骗 1 万元以下的有 25 人，受骗 1 万~2 万元的有 11 人，受骗 2 万~3 万元的有 4 人，受骗 3 万~4 万元的有 3 人，受骗 4 万~5 万元的有 4 人，5 万元以上的有 3 人，最多的一人被骗 9.13 万元。

事实上，退款诈骗是近年来非常流行的一种因网购信息泄露而引发的网络诈骗。骗子冒充客服，能够准确的说出受害者的网购信息，因此很据迷惑性。随后，骗子再通过发送虚假登陆的钓鱼网站或诱骗受害者主动转账等方式，诈骗受害者钱财。这种情况在其他电商主流电商平台上也时有发生。

三、 医疗卫生系统重大信息泄露事件

2017 年 4 月，浙江松阳警方侦破一起特大侵犯公民个人信息案件，查获非法获取的各类公民个人信息 7 亿余条，共 370 余 G 的电子数据。抓获犯罪嫌疑人 20 名，其中查获 2 名入侵相关信息系统的网络黑客。

经查，犯罪嫌疑人王某于 2016 年 2 月入侵某部委的医疗服务信息系统，将该系统数据库内的部分公民个人信息导出进行贩卖。

而李某则于 2016 年 9 月侵入某省扶贫网站，下载系统内大量公民个人信息数据贩卖，这些被贩卖的数据辗转又卖给了台湾等诈骗团伙。

第三章 国外机构重大信息泄露事件分析

本章主要介绍 2017 年，媒体报道的国外发生的一系列重大信息泄露事件，涉及军事、政府、金融、交通、互联网、医疗卫生、教育、传媒、旅游、酒店、餐饮等多个行业。总体来看，不同行业信息泄露的原因、信息泄露的内容以及信息泄露后的危害都有很大的不同。

一、 国外军事机构重大信息泄露事件

（一） 问题综述

军事机构的内部信息无疑是最为敏感的机密信息。在 2017 年媒体披露的军事机构重大泄密事件中，美国上榜次数最多，也是最受关注的。CIA、NSA、美国国防部，美国陆、海、空军等都未能幸免。

从国外军事机构机密信息泄露的原因和结果来看，主要有以下几个明显的特点：

- 1) 内鬼问题十分突出。斯诺登事件后，美国的军事机构中仍然不时出现内鬼。例如，前 NSA（美国国家安全局）承包商雇员马丁窃取了 NSA 超过 50 TB 的高度敏感数据。
- 2) 供应链安全问题十分突出。在下述的 7 个事件中，至少有三个事件可以明确是由于供应商、承包商或分包商的安全出了问题，从而导致了军事机构的信息泄露。
- 3) 网络武器成为攻击目标。在 2017 年，CIA、NSA 均发生了网络武器库泄密事件，相关代码被公布在互联网上以后，对普通公众的安全造成了极大的威胁。而 Wannacry，即永恒之蓝勒索蠕虫事件，更是将这种威胁放大了极致。
- 4) 低级运维错误仍普遍存在。比如，在下面举例的安全事件中，分别在 3 月和 11 月发生的两次军事数据库泄密事件，都与系统配置不当，缺乏有效的运维管理有关。

（二） 五角大楼分包商泄露机密的军事人员数据

2017 年 1 月曝出，五角大楼的分包商在互联网上暴露了大量在职军事医疗保健专业人士的高度敏感的信息细节，其中一些拥有最高机密的安全许可。数据泄露的许多受害者是美国特种作战司令部的工作人员，包括美国陆军，海军和空军等美国军方分支机构的前雇员。泄露的信息中包括姓名，合同类型，社会安全号码和税务起始日期等信息，以及详细说明工作人员不在现役时的生活区的方坯编号；这些信息最早可追溯到 1998 年。

波托马克医疗保健解决方案是一家分支机构，通过其驻华盛顿特区的承包商 Booz Allen Hamilton 向美国政府和军事组织提供医疗专业人员，是数据泄露的根源。

（三） 新加坡国防部 850 名用户数据泄露

2017 年 2 月，新加坡国防部在 I-net 系统（新加坡国防部内部使用的一种网络系统，可与互联网相连）中发现一次网络攻击行为，在此次攻击中被盗的数据包括 850 名受害人的身份证号码，电话号码和出生日期等信息。这些个人信息被用于管理用户帐户并存储在 I-net 上。

新加坡国防部要求所有受到影响的员工都必须更改 I-net 系统中的密码。同时，如果有人其他的网络系统中使用与 I-net 系统相同的密码，那么相关网络系统的密码也必须同时

修改。

（四） NSA 黑客部队 TAO 超过 75%的黑客工具被承包商雇员窃取

2017 年 2 月,《华盛顿邮报》报道了一起安全事件,一名前 NSA(美国国家安全局)承包商雇员马丁窃取了 NSA 超过 50 TB 的高度敏感数据,这些数据包含“获取特定情报行动办公室”(Tailored Access Operations,简称 TAO,)超过 75%的黑客工具。TAO 是 NSA 的精英黑客部门,负责开发并部署软件,用来渗透外国目标的计算机网络,从而实现间谍目标。

某匿名美国官员表示,马丁声称持有 TAO 超过 75%的黑客工具。扎卡里·A·梅尔斯表示,马丁拿走了“数千页”机密资料和 50 TB 的数字数据,其中许多具有“特殊处理说明”(指文件有通过特殊途径传递或仅供特定个人知悉等要求)。失窃的数据包含至少 5 亿页的政府档案,涵盖“国防”相关的机密信息。

（五） 美军泄露“安全通关文件”的“圣杯”

2017 年 3 月,安全研究人员发现,任何人都可以访问美国空军网络系统中千兆字节的文件,因为该系统与互联网连接的备份驱动器没有密码保护。不安全的备份驱动器已经暴露了数以千计的美国空军文件,包括高级官员的高度敏感的人事档案。

这些由 ZDNet 审查的文件包含了一系列个人信息,例如 4000 多名官员的姓名和地址,职级和社会安全号码。另一个文件列出了数百名其他官员的安全许可级别,其中一些人员拥有“最高机密”许可,并获得敏感的隔离信息和码字级许可。在其他几个电子表格中还可以找到工作人员的电话号码及其配偶的联系信息,以及其他一些敏感和私人的个人信息。

（六） CIA 泄露针对 Windows 系统的网络武器 Grasshopper

2017 年 4 月,维基解密公布了 Vault7 系列名为“Grasshopper”的 CIA(Central Intelligence Agency,美国中央情报局)网络工具相关文档,根据公布的文档显示,该工具主要针对 Windows 系统进行入侵控制,是一套具备模块化、扩展化、免杀和持久驻留的恶意软件综合平台。

在曝光的“Grasshopper”文档中,分为持久驻留机制说明、开发指导、系统设备测试、发行版本和设计架构六类共 27 份相关文件,这些文件主要对基于受害者客户端的恶意软件开发设计作出说明,其中包含的内幕信息侧面揭露了 CIA 的网络攻击入侵手段。

（七） 美国防承包商博思艾伦泄露五角大楼相关敏感文件

2017 年 6 月,网络安全公司 UpGuard 的网络风险分析师克里斯·维克里发现,来自美国国家地理空间情报局(简称 NGA)的某美国军方项目将超过 6 万份敏感文件存储于 Amazon 云存储服务器(美国规模最大的国防情报承包商之一的博思艾伦咨询公司存储)之上,且无需任何身份验证即可访问。这些文件中包含大量与美国政府系统相关的密码,而这些系统中存放有各类敏感信息以及博思艾伦咨询公司高层工作人员的安全凭证。更严重的是,这批泄露的文件中包含的数据甚至涉及本应受到高度保护的五角大楼系统管理访问权限的主凭证。

（八） 美军事数据库遭泄,网络监控数据曝光

2017 年 9 月,安全公司 UpGuard 的克里斯·维克里在亚马逊可公开访问的及数据库存储仓库中发现了美国陆军及 NSA 情报平台绝密文件。此事距离 UpGuard 发现美军中央司令部(CENTCOM)和太平洋司令部(PACOM)不安全 Amazon S3 存储桶的新闻爆发,甚至不到 2 周

时间。维克利发现的这个错误配置的 S3 存储桶，只要输入正确的 URL，任何人都能看到 AWS 子域名“inscom”上存储的内容。包含有 47 个文件和目录，其中 3 个甚至任由下载。UpGuard 称：“存储桶中的 3 个可下载文件，证实了这些内容的高度敏感性，暴露了国家安全数据，其中一些明显是机密的。”

2017 年 11 月，UpGuard 公司安全研究员克里斯·维克瑞表示，他发现三台隶属于美国国防部（简称 DoD），被错误配置的 Amazon S3 服务器，其中包含来自世界各地用户的 18 亿份社交媒体与论坛发帖，不少美国民众的言论信息也包含于其中。

根据克里斯·维克瑞的说法，数据库中的信息并不包含任何敏感细节。相反，这些数据库完全由收集自互联网的公开社交媒体帖子、论坛帖子、博客、新闻评论以及其它类似的信息片段拼凑而成。这批整理起来的数据包含帖子本体以及用于识别帖子的数据。大部分内容使用阿拉伯语、波斯语以及英语编写而成，且收集时间为 2009 年至 2017 年 8 月之间。

二、 国外政府机构重大信息泄露事件

（一） 问题综述

在 2017 年媒体公布的国外政府机构重大信息泄露事件中，美国和印度的上榜次数最多。总体来看，国外政府机构的信息泄露事件主要表现出以下几个明显特点：

1) 政府机构信息泄露的重要原因在于网络服务商或云服务商的管理疏失或安全漏洞。这也再次说明政务云系统的云服务与安全服务分开管理的必要性。如果政府机构只是简单的把业务系统托管给网络服务商或云服务商，而没有引入第三方的专业安全管控，那么信息泄露的风险就会大大增加。

2) 超大规模的信息泄露事件频发，泄露信息数量动辄上千万。例如，2017 年，美国和印度就都爆发了政府机构过千万，甚至过亿条公民信息的大规模泄露的事件。而英国爱丁堡发生的信息泄露事件，甚至影响到了当地近 1/4 的人口。

3) 政府机构泄露的公民个人信息往往是综合性信息，包括姓名、身份 ID（如身份证号码）、家庭住址、家庭关系、工作情况、电话号码和电子邮箱等。而这些详细的个人资料在各国都被普遍的用于实施精准的网络诈骗。

（二） 黑客入侵 FBI 网站，公开 FBI.gov 用户敏感信息

根据国外媒体的最新报道，2017 年 1 月，臭名昭著的黑客 CyberZeist (@cyberzeist2) 成功入侵了美国联邦调查局的官方网站 FBI.gov，并将该网站中的部分数据发布到了 Pastebin 网站上。此次泄露的数据中包括 FBI.gov 的用户账号信息，其中包括账号的用户名、SHA1 加密的用户密码、SHA1 盐值、以及用户邮箱等信息。

根据安全研究专家透露的信息，CyberZeist 从 FBI.gov 的服务器中发现了几个备份文件（acc_102016.bck、acc_112016.bck 和 old_acc16.bck 等等），并在这些备份文件中找到了大量用户数据。

（三） 黑客组织利用 El Machete 窃取全球政府超过 100G 数据

2017 年 3 月消息，某黑客组织目前正针对全球知名政府组织机构展开攻击。该黑客组织使用定制恶意软件“El Machete”持续发起攻击，并通过社会工程学技术进行传播，目前已经窃取了超过 100G 的数据。

安全研究人员认为,该黑客组织将主要目标锁定在拉丁美洲,此外还针对加拿大、英国、德国、韩国、俄罗斯、乌克兰和美国的组织机构展开攻击。安全公司 Cylance 的安全研究人员确定 El Machete 是一款定制恶意软件,其严重依赖 Windows API,旨在逃避传统反病毒软件的检测,该黑客组织瞄准的是“高价值”目标,包括情报机构、军事和政府组织机构。

(四) 印度 1.35 亿公民身份信息和 1 亿条银行账户信息被泄露

2017 年 5 月,根据印度互联网与社会中心(简称 CIS)发布的一份题为《Aadhaar 信息安全实践(抑或缺失): Aadhaar 号码中敏感个人财务信息文件的公开可用性》的报告所述,此类系统中出现的任何问题都将引发毁灭性的灾难,强调了 Aadhaar 本身所采取的高安全性保障机制,同时警告允许其它政府机构访问该系统可能导致数据泄露。

Aadhaar 是印度政府强制推行的全国性生物识别项目。每个印度公民都拥有一个独一无二由 12 位数字组成的 Aadhaar 号码,它的背后存储的是每个人的生物特征数据以及个人身份信息。数据显示,目前约有 1.35 亿条 Aadhaar 号码及 1 亿条银行账户号码可能已经由负责处理政府养老金及农村就业项目的门户网站处外泄。

2017 年 11 月,印度又发生了一起严重的数据泄露事件。隶属于印度中央政府和邦政府(包括教育部门)的 210 个网站公开暴露了部分印度公民的个人信息,包括他们的姓名、地址、Aadhaar 号码和其他信息。其中,最引人关注的还是 Aadhaar 号码。

(五) 美国 9 州选民登记数据暗网销售——千万记录仅售 4 美元

2017 年 7 月,威胁情报公司 LookingGlass Cyber Solutions 称,美国近千万选民记录在暗网上仅售 4 美元(约合 27 元),美国 9 大州超过 4000 万选民的被窃信用卡数据和登录凭证在地下论坛进行交易。被售卖的选民记录包括:选民的全名、选民 ID、出生日期、选民身份、所属党派、居住地址和其它详情。选民涉及美国 9 大洲:阿肯色州、科罗拉多州、康涅狄格州、特拉华州、佛罗里达州、密歇根州、俄亥俄州、俄克拉何马州和华盛顿州的选民。

(六) 英国爱丁堡超过 11 万公民个人信息流入暗网

2017 年 7 月,黑客在暗网出售逾 11 万条爱丁堡公民个人信息,此次泄露数据约占其总人口数(据 2014 年统计,爱丁堡总人口约 464,990)的 24%。被泄露信息包括公民电子邮件用户名、密码与信用卡数据等。

伦敦数据公司 C6 在对事件展开调查后发现,与 EH1、EH4 邮编有关的公民身份信息窃取案例共计 115333 宗,是骗局中受影响程度最为严重的部分。

(七) 亚马逊 AWS 服务器信息泄露 180 万选民信息被曝光

2017 年 8 月,美国一家选票计算机公司上周四证实,他们泄露了 180 多万伊利诺伊州居民的个人信息。而泄露的信息中包含选民姓名、地址、出生日期、部分社会安全号和部分党派关系,此外还包含一些驾驶执照和州身份证信息。网络安全公司 UpGuard 的乔·亨得利在一台未受密码保护的亚马逊网络服务(AWS)设备上发现了此项漏洞。磁盘分析师克里斯·维客利随后下载了这些选票数据,并判断这些数据来自 Election Systems & Software(以下简称“ES&S”)——这家公司为至少 42 个州提供选票计算机和服务。

(八) 印度国家互联网注册机构(IRINN)遭入侵,数据库在暗网兜售

2017 年 10 月,seQtree 和 Seqrite 团队的安全研究人员注意到在暗网中的某个论坛上,有黑客在兜售一个印度国家互联网注册机构 IRINN(Indian Registry for Internet Names and

Numbers, 是 India's National Internet Registry 的别称) 的数据库信息, 主要包括: 用户名、电子邮件 ID、密码、组织名称、发票/账单文档以及其他一些重要的字段, 最可怕的是, 黑客甚至可以操作 IP 地址的分配。此次事件在印度国内影响的范围广泛, 包括印度国家身份识别管理局、国防研究与发展组织、电信、万事达卡/Visa、印度国家银行等 6000 多家互联网服务提供商、政府机构和私营企业的信息。

(九) 南非史上最大的数据泄露事件 三千万公民信息泄露

2017 年 10 月, 知名安全专家 Troy Hunt 披露了南非史上最大的数据泄露事件。南非共 3 千万公民 ID 号及其他个人信息在网上泄露, 大量关于南非公民的敏感信息, 包括身份证号、个人收入、年龄、就业经历、民族、婚姻情况、职业、地址和雇主信息等。

这些数据泄露的时间跨度非常长, 从上世纪 90 年代初一直到现在。对数据文件进行分析后可以得出, 此次信息泄露的发生时间是在 2015 年 4 月。据网站 iafrikan.com 的社论人士介绍, 泄露数据的来源是 Dracore Data Sciences 的 GoVault 平台, 其客户 TransUnion 是南非最大的信用机构之一。

(十) 首例盗用总统信息的犯罪活动: 阿根廷总统成“毒贩”

2017 年 10 月消息, 阿根廷安全部接到网民举报, 称当地一网店大肆贩卖禁止零售的精神类药品和大麻、可卡因等制品。经警方调查, 居然发现该网店注册人信息显示的是阿根廷总统马克里。安全部门立即通过注册的 IP 地址和用于交易的联系电话锁定犯罪嫌疑人所在地。在距阿根廷首都布宜诺斯艾利斯以西约 40 公里一处小镇抓获涉案的兄弟二人, 并查获了大批制毒原料和作案工具。

阿根廷总统马克里是商人出身, 曾担任足球俱乐部主席和布宜诺斯艾利斯市市长, 因此其身份证号码、个人税号等相关个人信息在一些当地网站上均可查到。

三、 国外金融行业重大信息泄露事件

(一) 问题综述

2017 年, 国外金融机构的信息泄露事件主要表现为以下几个特点值得关注:

1) 信息泄露伴随财产损失。与其他机构的信息泄露不同, 金融机构的信息泄露往往会伴随更为直接的重大财产损失。2017 年, 就至少发生过两次俄罗斯黑客通过大规模窃取金融机构用户账户, 进而非法盗取钱财的攻击事件发生。。

2) 误操作也可能引起重大损失。即便是在安全管理相对较严, 安全措施相对较多, 安全级别相对较高的金融机构, 也同样会发生因操作失误导致的重大事故。富国银行的一名员工就因为误发一封邮件, 结果泄露了近 5 万名客户的个人信息。

3) 内鬼问题和技术窃密值得关注。例如, 2017 年 4 月曝出的黑客内鬼窃取华尔街金融服务公司核心交易算法事件, 使我们有理由担忧, 防范严密的金融机构也极有可能从内部被攻破。

此外, 2017 年 6 月, 美国最大的医疗保险公司 Anthem 已经同意支付 1.15 亿美元来解决 2015 年数据泄露带来的集体诉讼。这一事件对于国内网络安全法落地实践, 对于如何就政企机构因网络安全事件造成普通公民经济损失问题追究其法律责任, 具有一定的参考意义。

（二） 日本 10 万条信用卡信息泄露 支付服务提供商被问责

2017 年 3 月，日本支付服务提供商 GMOPayment Gateway（GMO PG）公司证实，黑客利用其应用框架中的 Apache Struts2 漏洞对该公司的两大客户的网站发起攻击，并导致大量个人数据被窃。这两大客户分别为东京都政府和日本住宅金融支援机构。

通过东京都政府网站泄露的数据量为 67.6 万条，包括 61.5 万条电子邮箱地址、6.17 万条信用卡号以及信用卡到期日。从日本住宅金融支援机构泄露信用卡信息为 4.35 万条，包括信用卡号、信用卡到期日、安全码、信用卡支付注册日期、地址、电子邮箱地址、姓名、电话、出生日期和支付加入日期等。

（三） 俄罗斯与亚美尼亚黑客联手从澳大利亚多家银行窃取约 18 万美元

2017 年 3 月消息，亚美尼亚国家安全委员会发布的消息称：“自 2016 年 8 月到 12 月，一个由俄罗斯与亚美尼亚公民组建的网络犯罪集团成员总计从澳大利亚银行客户的帐户中窃取约 8500 万德拉姆（约 18 万美元）。不过由于亚美尼亚国家安全委员会实施了广泛调查与情报追踪举措，犯罪集团已经被发现且相关行为得到遏制。”

根据初步数据，该犯罪集团成员以酒店与餐厅经营等借口在 Armenia 3 贸易组织中进行注册，并借此获取终端收银机。在此之后，他们得以通过输入银行卡数据进行非现金交易，而不再需要获得持卡人及其银行卡的详细信息。

（四） 信贷公司 Wonga 数十万客户数据被泄

2017 年 4 月，英国知名的发薪日贷款（Payday Loan）公司 Wonga 确定遭遇数据泄露，并发表声明通知客户联系银行。Wonga 在声明中指出，黑客可能非法访问了数十万账户的个人信息，关系到预计总计高达 27 万客户数量的个人信息。本次泄露的信息可能包括：客户姓名、电子邮箱、家庭住址、电话号码、银行卡的后四位数、银行卡账号和银行代码。唯一庆幸的是，黑客并未窃取到完整的银行卡信息。

（五） 黑客内鬼窃取华尔街金融服务公司核心交易算法

2017 年 4 月，一名曾在华尔街一家市值数十亿美元的金融服务公司（KCG 控股公司）工作的某高级系统管理员被 FBI 指控，原因是这名男子开发恶意软件窃取了有价值的源代码和加密密钥，而且直接访问了该公司核心业务的数据文件。

他被指控窃取超过 300 万个机密和专有文件，而这些文件是 KCG 业务的核心，这些文件帮助该公司在 2016 年赚取超过 14 亿美元的收入。据了解，该男子还曾在 KCG 控股公司的圣何塞办事处工作长达 7 年之久。

（六） 俄罗斯黑客入侵 100 多万部安卓手机 盗取银行客户 5000 多万卢布

2017 年 5 月，俄罗斯官员宣布，他们已经成功打击了一个专门盗取银行账户资金的黑客组织。他们通过恶意软件 Cron 感染了俄罗斯 100 多万部 Android 手机，并盗取了银行客户超过 5000 多万卢布（约合人民币 609 万元）。

基于 Android 的恶意软件 Cron 感染用户的手机后，允许黑客向受害者的银行发送短信，并要求其向每个受害者平均转出 140 美元，病毒将会在被感染的手机上隐藏来自银行的所有通知。到目前为止，Cron 已经将资金存入 6000 个黑客银行帐户。

（七） Anthem 同意支付 1.15 亿美元解决 2015 年数据泄露带来的集体诉讼

2017 年 6 月消息，美国最大的医疗保险公司 Anthem 已经同意支付 1.15 亿美元来解决 2015 年数据泄露带来的集体诉讼。2015 年，针对 Anthem 的网络袭击（定制的恶意软件被用来渗透 Anthem 的网络并窃取数据）泄露了 7880 万条用户记录，记录包括保险人的姓名，出生日期，地址和医疗身份证号码，但保险人的财务信息和医疗记录没有被泄露。

类似的，2017 年 3 月，美国零售巨头 Target 也与美国总检察长达成和解协议，并同意在 2013 年的数据泄露事件中支付 1850 万美元。

（八） 富国银行发错电子邮件 导致 5 万客户信息泄露

2017 年 7 月，前理财顾问加里·辛德布兰德（Gary Sinderbrand）正在对美国富国银行一名员工提起诽谤诉讼，他原本会收到与本案相关的电子邮件和其他文件，然而富国银行却向他发送了 1.4GB 包含 5 万名高净值客户信息的数据，包括姓名、财务信息，以及社会安全号码等。报道称，受影响客户的投资资产达到数百亿美元，更糟糕的是，辛德布兰德的律师收到的这些数据并没有附以保密协议，或是由法官签署的保护令。

（九） 信用机构 Equifax 遭黑客攻击，1.43 亿用户信息泄露

2017 年 9 月，美国信用机构 Equifax 被证实在今年 5 月到 7 月期间遭到黑客攻击，导致约有 1.43 亿用户数据遭到泄露。事件曝光后，Equifax 股票暴跌 30%，相当于蒸发掉 50 亿美元市值。Equifax 黑客事件位列史上罕见大型数据泄露事件之一，被盗记录中包含社会安全号、驾照信息、信用卡号、姓名和住址等。

（十） 支付管理公司 TIO Networks 遭黑客入侵 泄露了 160 万用户信息

2017 年 12 月，PayPal 发布的信息表示，该公司在今年早些收购的支付管理公司 TIO Networks 遭遇了网络安全事件，在此期间，攻击者似乎访问了 160 万用户存储信息的服务器。在事件发生后，PayPal 于 11 月 10 日暂停了 TIO Networks 的所有业务，并开始了内部调查。

该公司并没有透露攻击者访问了什么类型的信息。但由于这是一个支付系统，安全专家表示，这些信息可能不仅包含了 TIO Networks 用户的账户和密码，还包含了个人信息（PII）和财务细节。

目前，TIO Networks 正在逐一通知受影响的用户，并开始与消费者信用报告机构合作，为这些用户提供免费的信用监控服务。

四、 交通行业重大信息泄露事件

（一） 问题综述

2017 年，交通行业发生重大信息泄露事件的机构主要集中在民航和汽车领域。泄密原因多种多样。其中也有一些高级机密信息泄露的事件发生，如英国女王安保路线这样高度机密的信息被泄露等。

（二） 纽约机场敏感数据遭泄露 机场安全故障目录曝光

2017 年 2 月消息，纽约州北部机场发生重大信息泄露事件，数据曝光后泄露的敏感文件显示：近年来，机场系统出现过几个重大安全漏洞。在 ZDNet 上可以看到的数十个

文件列出了在曼哈顿以北大约 60 英里的斯图尔特国际机场过去几年的安全漏洞目录。

斯图尔特国际机场每年为数十万乘客提供服务，其中包括备受瞩目的客人和私人包机。例如，ZDNet 看到的文件显示，2010 年机场工作人员在未知的一段时间内无法屏蔽美国政府禁止在其领空飞行的恐怖分子嫌疑人的名单。

（三） 遗弃 U 盘里竟有英国机场安保机密，包含英女王抵达路线

2017 年 10 月，一名无业男子在伦敦某街道找到一个 USB 闪存盘，里面有地图、视频和文件，它们涉及希思罗机场安全保障和反恐行动。甚至，某份文件中有预防恐袭的机场巡逻路线，另一份文件中有英国女王伊丽莎白二世抵达机场的路线以及保护她所采取的措施。这名男子把 U 盘交给《星期天镜报》，该报把 U 盘转交给机场人士。

（四） 1000 万辆汽车 VIN 识别码数据被泄，小心买到克隆车

2017 年 6 月，据媒体报道，已经发现一个汽车数据库被泄露至网络当中，数据库囊括美国本土出售的上千万辆汽车以及相关购买者的个人信息。受这起泄露影响的汽车经销商包括 Acura(讴歌)、BMW（宝马）、Chrysler（克莱斯勒）、Honda（本田）、Hyundai（现代）、Infiniti（英菲尼迪）、Jeep（吉普）、Kia（起亚）、Mini（迷你）、Mitsubishi（三菱）、Nissan（尼桑）、Porsche（保时捷）和 Toyota（丰田）。

这套未受保护的数据库由 Kromtech 安全研究中心的研究人员们所发现，其中共包含以下三组数据：车辆细节信息：车辆识别编码（简称 VIN）、制造商、型号、型号年份、车辆颜色、里程数等。销售细节信息：VIN、里程表、销售总额、付款方式、每月付款金额、购买价格、支付方式等。客户细节信息：全名、地址、手机/家庭/工作电话、电子邮件、出生日期、性别、职业等。

（五） Uber 被指向黑客低头，曾花 10 万美元平息盗号风波

2017 年 11 月，Uber 公司被爆曾在 2016 年 10 月被黑客攻击，致使 5700 多万用户和司机账号被盗。消息称，Uber 对外隐瞒了这一事件。并且支付了 10 万美元，要求黑客删除数据。事件发生后，Uber 调整了安全措施避免再受攻击，但并未明确这一事件的责任人是谁。

五、 国外互联网企业重大信息泄露事件

（一） 问题综述

互联网企业往往服务用户众多，信息系统复杂，同时互联网领域也是信息泄露事件最为频发的领域之一。从 2017 年互联网企业重大信息泄露事件来看，主要表现出以下几个特点值得关注：

1) 帐号密码仍然是互联网企业信息泄露的主要形式，其中，电子邮箱和网络游戏的账户最受攻击者关注。

2) 技术资料泄密事件多发，并可能引发难以估计的损失。如微软的源代码泄露事件、Hadoop 服务器泄密事件，都有可能引发攻击者恶意使用相关代码，或发现代码中隐藏的更多安全漏洞。

3) 互联网企业的安全漏洞或管理疏失，往往会殃及大量使用这些互联网企业服务的企业和个人。如 2017 年 7 月的 Google 网上论坛泄密事件，就直接导致了数百家企业的商业机

密泄露。

4) 物联网服务可能引发的信息泄露成为现实。其中最典型的例子就是泰迪熊泄密事件。

(二) 互联网连接泰迪熊泄露数以百万计的语音信息和密码

2017 年 2 月, 网络安全研究员 Troy Hunt 提供的一份调查报告指出, 从去年 12 月 25 日到 2017 年 1 月 7 日, “云宠物”的超过 82 万个用户的帐户被泄露, 其中包括 220 万条语言信息。

出事的是来自品牌“云宠物”(CloudPets)的泰迪熊(teddy bears), 一款可以连接互联网的智能玩具。报告指出:“云宠物”的制造商把用户的数据储存在一个任何人不需要身份认证和密码就可以访问的云端数据库中, 导致大量数据信息, 包括用户的姓名、地址、电子邮箱及密码被多次查看, 甚至被网络罪犯盗走。现在网上已经出现几个帖子, 对“云宠物”用户进行敲诈勒索, 要求用户付钱赎回被犯罪分子恶意储存的语音文件。

此前, 也曾有德国监管机构要求消费者立即停止使用品牌为“我的朋友 Cayla”(My Friend Cayla)的洋娃娃, 因为担忧玩具体内的联网设备可能被别有用心黑客用来监视儿童和家长。现在这种担忧在美国变成了可怕现实。

(三) 雅虎泄露 3200 万账户数据

2017 年 3 月, 雅虎公布的消息显示: 在过去两年间, 有入侵者进行“Cookie 伪造”攻击, 造成 3200 万账户信息泄露。

通过 Cookie 伪造攻击, 攻击者在无需输入密码的情况下, 就能访问受害者账户, 只需伪造一个 Web 浏览器 token, 即 Cookie 来诱使浏览器相信雅虎用户已经登录。从 2017 年 2 月开始, 雅虎就开始警告其用户可能被入侵, 并陈述用户可能被窃取的信息包括姓名、邮箱、哈希密码、电话号码、生日和一些加密或者未加密的安全问题和答案。

2017 年 11 月, 受大量账户信息泄露事件困扰的雅虎和 Equifax 公司高管玛丽莎·梅耶尔(Marissa Mayer)和里克·史密斯(Rick Smith)对账户泄露事件致歉, 并表示他们仍然在寻求解决方案。

(四) DaFont 网站遭到黑客攻击, 近 700,000 个账户被暴露

2017 年 5 月, DaFont.com(提供各种文字编辑字体服务)宣布, 该网站当月早些时候遭到黑客入侵, 以明文形式暴露了近 700,000 个用户账户的数据库。该数据库不仅包含用户名, 电子邮件地址和密码, 还包含从论坛收集的数据和用户对话, 以及来自美国和英国的 Microsoft, Google, Apple 和政府机构的公司帐户。数据库的详细信息可以在 Troy Hunt(知名安全专家)的“Have I Been Pwned”网站上找到。对数据库的分析显示, 在数据库中有 637,340 个唯一的电子邮件地址, 其中 62%的电子邮件地址已经被其他黑客利用。

(五) 游戏《Cyberpunk 2077》文件遭黑客窃取

2017 年 6 月, CD 新作《Cyberpunk 2077》的一些内部文件和概念设计被黑客窃取并被用以勒索。黑客们已经向 CD 提出赎金要求, 宣称如果得不到满足的话, 他们就会在网上公开《Cyberpunk 2077》的开发资料。不过针对此事件, CD 的开发人员好像并不担心: 窃取事件所涉及的文件是老版本, 在很大程度上并不能代表当前版本的游戏。

今年早些时候, 该公司的官方论坛遭到黑客攻击, 约有 190 万用户帐户被曝光, CD 的

开发人员表示，这些帐户源自公司的旧版数据库，早在 2016 年 3 月就曾遭遇过入侵。

（六） Hadoop 服务器配置不当致使全球 5120TB 数据泄露

2017 年 6 月，根据使用 Shodan 搜索引擎进行的分析结果发现，配置 Hadoop 分布式文件系统（HDFS，Hadoop 应用程序使用的主要分布式存储）的近 4500 台服务器，已经暴露了超过 5120TB（5.12PB）的数据。此次泄露事件也是出于一个相同的问题——基于 HDFS 的服务器（主要是 Hadoop 安装）缺乏安全配置。作为此次泄露事件的主角，大多的 HDFS 服务器主要位于美国（1900 台）和中国（1426 台），其次是德国（129 台）和韩国（115 台）。中国也受到巨大的影响。

（七） 微软官方确认部分 Windows 10 源码被泄露 容量大约 1.2GB

2017 年 6 月，微软 Windows 10 源代码的一部分被泄露到了追踪 Windows 版本的爱好者网站 Beta Archive 上，微软在经过调查后向外媒 The Verge 确认，确实有来自共享源计划源代码的一部分被泄露，这些代码主要提供给 OEM 合作伙伴使用。此前有消息称大约 32TB 的数据被泄露，但实际上此次泄露的规模相对较小，大约 1.2GB。此次泄露的源码内容涉及 Windows 10 Mobile Adaption Kit、部分 Windows 10 Creators 以及 ARM Windows 10 版本的代码。

（八） Google 网上论坛配置错误导致数百家企业机密数据在线曝光

2017 年 7 月，安全公司 RedLock 研究人员发现 Google Groups 在线服务出现配置错误，导致 IBM' s Weather Company、Fusion Media Group、协助桌面支持服务提供商 Freshworks 与视频广告平台 SpotX 等数百家企业机密数据在线曝光。RedLock 研究人员发现，此次事件致使受害企业员工电子邮件地址与内容，以及员工薪酬补偿、销售渠道数据、客户密码、姓名与家庭地址等个人身份信息在线泄露，可供全球用户任意查看。

值得深思的是，引发这起数据泄露事件并非安全漏洞，仅是 Google Groups 功能设置不当。但这一事件表明，任何一次操作疏忽都将对企业产生毁灭性影响，一旦网络犯罪分子获取这些企业信息，就可用来劫持企业帐户、开展网络钓鱼攻击以及在线泄露敏感谈话内容等。

（九） 瑞典大型网络托管公司遭黑客“拖库”，其数十万客户受影响

2017 年 8 月，瑞典大型网站托管公司 Loopia 遭黑客“拖库”，客户数据外泄。Loopia 发表声明称，攻击发生在 8 月 22 日，黑客访问了部分客户数据库，包括 Loopia Kundzon 的个人资料、联系信息和加密（哈希）密码。Loopia 信用卡等支付信息未泄露，客户的托管网站和电子邮件服务未遭受攻击。为了进一步确保安全，该公司修改了所有客户的账户号和密码，并通知了客户，建议重置系统密码并更新个人信息。

（十） 微软储存内部漏洞的秘密数据库 4 年前就被黑客偷走

2017 年 10 月，5 名微软前员工透露，微软储存自家软件内部漏洞的秘密数据库早在 4 年以前就被一伙组织严密的黑客盗走，数据库包含了一批世界范围内使用的软件的关键未修复漏洞，包括 Windows 操作系统。

在知晓此次攻击后，微软曾发动调查，并没有发现利用该数据库信息进行攻击的行为。5 名前员工对上述调查结果持不同意见，两名员工认可了这一结论，另外三名员工认为，调查样本太少，不足以支持该结论。在此次事件发生后，微软将这一数据库从公司网络中隔离，并且需要通过两步验证措施才能访问。

（十一）Imgur 承认 2014 年遭黑客攻击，170 万账号信息被窃取

2017 年 11 月，全球知名图片分享网站 Imgur 对外承认，2014 年该网站曾经受到黑客攻击，170 万包含邮箱地址和密码的账户信息被窃取。Imgur 表示，由于网站并不需要用户提交真实姓名、地址或者手机号码，因此被窃取的信息中并不包含私人信息。

六、 医疗卫生机构重大信息泄露事件

（一） 问题综述

医疗卫生行业的信息泄露一般可以分为病患信息泄露和医院信息泄露两个方面。而这两方面的信息泄露事件，在 2017 年均有发生。特别让人担忧的是，病患信息属于极其敏感的个人信息，知名人士病患信息的泄露甚至可能引发社会不安。

（二） 黑客入侵英国顶级整形医院数据库：盗取大量私照

2017 年 10 月，据 Daily Beast 网站报道，黑客组织 Dark Overlord 宣称他们攻入了全球知名整形美容医院 London Bridge Plastic Surgery (LBPS) 的数据库，获取了大量的隐秘信息。这些资料中包含有病人的名字、住址等信息，更关键的是还有很多生殖整形、丰胸等手术的私照，其中除了普通人，还有英皇室成员和明星艺人，容量高达 TB 级。

（三） 黑客窃取数千名医院工作人员的个人数据

2017 年 3 月，黑客窃取了数千名 NHS (National Health Service, 即英国国家医疗服务体系) 医疗专业人员的信息，这是通过入侵其私营承包商的服务器来实现的。网络攻击者渗透到由 IT 供应商 Landauer 运营的数据服务器中，窃取了数千名医疗工作人员的姓名，出生日期，辐射剂量和国家保险人数等信息。

英国加的夫的 Velindre NHS Trust 通过 Velindre 癌症中心为威尔士各地的卫生局提供辐射检查服务。在发给 ZDNet 的一封电子邮件中，该信托机构证实，自己的员工中有 530 人受到了此次攻击事件的影响，并已联系到所有相关人员。

七、 教育机构重大信息泄露时间

（一） 英国学生化身黑客窃取考试答案，分数太高被发现

2017 年 2 月，就读于位于英国埃尔市的一所高中学校的五名学生，在考试前他们通过黑客手段窃取了老师邮箱的用户名和密码，进入邮箱拿到了数学考试的答案。之后几名学生对着这份答案“潜心苦读”，最终交上了一份“近乎完美”的答卷。但老师在阅卷时发现了这几份试卷存在异常，所得分数与这几名学生的平时水平不符。随后学校和老师对此事展开了调查，将几名“黑客”抓获。

（二） 罗格斯大学遭遇数据安全事件 1.7 万学生信息意外在线暴露

2017 年 12 月，美国罗格斯大学的官员证实，1700 名罗格斯学生的学术信息在 2017 年 11 月 8 日和 9 日的数据安全事件中遭到了在线暴露。

罗格斯大学发言人 Neal Buccino 强调，暴露的数据不包括任何人的社会安全号码 (Social Security number, SSN)、家庭住址或财务信息。

Buccino 解释说，暴露的数据来自计算机科学学生的学术资料，包括 Rutgers ID 号码、GPA 和 2018 年春季课程表。

Buccino 说，此次事件的发生来源于管理失误，罗格斯大学目前正在更新相关的安全策略，以确保此类事件不会再发生。

八、 传媒机构重大信息泄露事件

（一） 问题综述

2017 年发生的，国外传媒机构重大信息泄露事件大多与黑客攻击有关，也有个别情况是由于运维不当造成的。媒体机构泄露信息的内容也是多种多样。有的是泄露了用户信息，有的是泄露了商业机密，有的则是泄露了尚未发布的内容资源——这对于专门从事影视或内容制作的传媒机构来说是致命的。

值得一提的是，由于媒体或多或少的会存在一定的政治属性，所以，在针对媒体的网络攻击中，不能忽视政治因素。

（二） 黑客通过麦克风窃取乌克兰 70 目标超 600G 数据

2017 年 2 月，工业网络安全公司 CyberX 发现了一个大规模的网络攻击行动，该行动瞄准了乌克兰的很多目标，至少已经成功入侵了 70 个目标，涉及到关键基础设施、媒体和科学研究机构。该行动的目的是捕捉目标中的一系列敏感信息，包括对话录音、屏幕截图、文件和密码。由于它能偷偷摸摸的在目标系统中植入窃听程序，窃取敏感音频，并使用 Dropbox 来存储偷取的数据，因此 CyberX 将它命名为“Operation BugDrop”。

（三） 《华尔街日报》母公司道琼斯 220 万客户信息外泄

7 月 19 日讯，网络安全公司 UpGuard 的网络风险小组发布报告指出，由世界一流的商业财经信息提供商、新闻媒体出版集团道琼斯公司持有的一套云文件存储库存在配置错误，且其中包含的来自数百万家企业客户的个人及财务敏感信息以半公开形式接受网络访问。尽管道琼斯方面证实至少有 220 万客户受到影响，但根据 UpGuard 方面的计算，受影响客户量可能接近 400 万。

此次泄露的数据包括《华尔街日报》以及《巴伦周刊》在内的各道琼斯公司出版物的数百万名订阅者的姓名、地址、帐户信息、电子邮件地址以及信用卡后四位号码。另外，此次一同被暴露在云端的还有“道琼斯风险与合规”系列数据库当中的 160 万条记录，这些数据库属于一个仅供企业订阅的情报项目，用以帮助各金融机构遵循法规以打击洗钱活动。

（四） HBO 安全承包商：黑客盗走了上千份公司内部文件

据外媒报道，2017 年 8 月，受雇于 HBO 的安全公司 IP Echelon 表示，HBO 遭遇了网络攻击，黑客偷走了这家公司上千份内部文件。截止到目前为止，黑客已经公布了《投手》、《104 号房间》的剧集内容、《权力的游戏》的剧本以及两集要等到明年才会播出的喜剧剧集《巴里(Barry)》。

另外，黑客似乎还泄露了一名高管的个人信息，其以文本文件的形式公布在了网上，里边包含了数十个网络账号登录信息。在这些账号中，至少有一个可以让黑客获取该名高管的工作邮箱。实际上，黑客已经承认他们拥有访问 HBO 关键网络基础设施的权限并且从中盗走了 1.5TB 的数据，未来他们将可能将这些信息公布到网上。

九、 旅行、酒店及餐饮业的重大信息泄露事件

（一） 问题综述

2017 年，针对旅行社、酒店及餐饮行业的网络攻击也频繁发生。这些攻击主要有以下几个明显的特点：

1) 针对终端刷卡设备，特别是 POS 机的恶意程序攻击，已经成为一种盗取信用卡信息、进而盗刷用户信用卡的主要手段之一。相关技术手段已经十分成熟。

2) 旅行、酒店及餐饮等机构普遍缺乏必要的网络安全管理措施，服务器系统极易遭到入侵和破坏。

3) 相比于其他行业机构的信息泄露，旅行、酒店及餐饮行业的信息泄露包括大量的用户生活、出行等隐私信息。

（二） ABTA 网站遭到黑客攻击，4.3 万人受到违规影响

2017 年 3 月，ABTA（英国旅行社协会，Association of British Travel Agents）首席执行官马克·坦泽表示，“外部渗透者”使用公司网络服务器中的一个漏洞来访问其成员和一些成员客户提供的数据。该时间可能已经影响了 43,000 个人。大约 1000 个访问的文件可能包括与 ABTA 成员的客户有关的个人身份信息，这些信息是为了支持他们对 ABTA 成员的投诉而提交的。这些档案涉及 2017 年 1 月 11 日之后上传至 ABTA 的投诉。

（三） 洲际酒店集团二度遭遇信用卡数据泄露，超过 1000 家酒店受影响

2017 年 4 月，洲际酒店集团公布，该集团旗下逾 1000 家酒店遭遇信用卡数据泄露。客户在受影响酒店进行信用卡支付后，该恶意程序从信用卡磁条中读取记录数据，包括信用卡号码、有效期、内部验证码，有些情况下还包括持卡人姓名。酒店表示其他信息并未受到影响。

这是洲际酒店第二次发生信用卡数据泄露。今年早些时候，集团曾告知其客户，2016 年 8 月至 12 月在美国 12 家 IHG 酒店的餐厅及酒吧使用的信用卡数据遭泄露。当时受影响的酒店包括旧金山洲际酒店、阿鲁巴岛假日酒店、芝加哥华丽一英里洲际酒店等。

（四） 近 40 家 Shoney's 餐厅信用卡信息泄露

2017 年 4 月，Best American Hospitality Copr（BAHC）公司收到一份报告，这份报告指出网络犯罪团伙通过在其 PoS 系统上植入恶意软件，成功窃取了近 40 家 Shoney's 餐厅的信用卡数据——Shoney's 是位于田纳西州的全美家庭式餐厅。

BAHC 聘请 Kroll Cyber Security 安全公司来调查这起事件。这家安全公司证实，黑客在数十家 Shoney's 餐厅的支付处理系统上均远程安装了恶意软件，恶意软件感染设备后，它的主要目的是窃取持卡人的姓名，卡号，到期日期和内部验证码等数据。调查显示，一些受影响的餐厅是在 2016 年 12 月 27 日遭遇数据泄露的，而其他受影响的地点则于 2017 年 1 月 11 日首次遭遇数据泄露。

（五） 必胜客官网遭入侵，支付卡信息可能泄露

2017 年 10 月，美国必胜客通知其顾客，由于网站遭到临时入侵，他们的支付卡信息和联系信息可能被盗。黑客在 2017 年 10 月 1 日至 10 月 2 日之间进入该网站，总共约 28 小

时。在此期间，使用必胜客网站或移动应用预订订单的用户可能会受到影响。这一漏洞很快被发现并得到了解决，估计在此期间不到 1% 的网站访问受到影响，美国大约有 6 万人受到了这一事件的影响。其外部网络安全顾问确定攻击者可能已经获得了诸如姓名、账单、邮政编码、送货地址、电子邮件地址和支付卡等信息，包括卡号、有效期和 CVV。

（六） 凯悦酒店被黑客攻击，中国 18 家住客信息再遭泄露

据《北京商报》报道，10 月 17 日，全球 11 个国家的 41 家凯悦酒店支付系统被黑客入侵，大量数据外泄，包括住客支付卡姓名、卡号、到期日期和验证码。据报道，国内共有 18 家凯悦酒店受到影响，是这次事件中受影响最大、数量最多的国家。

调查显示，这些未经授权访问的客户支付卡数据，是从 3 月 18 日至 7 月 2 日之间的在一些凯悦管理地点的前台，通过手工方式输入或刷卡的。导致这次事件的原因，就是来自第三方含有恶意软件代码的卡片。黑客通过卡片上的恶意代码，入侵到酒店 IT 系统，通过酒店管理系统的漏洞，获取数据库的访问权限，提取与解密后，获得用户的私人信息。

十、 其他重大信息泄露事件

（一） 美国 52GB 个人身份信息泄露

2017 年 3 月，网络安全专家兼微软区域主管 Troy Hunt 在博客上披露了他收到的一份多达 52GB 的数据库资料，内容包含近 3400 万美国人的个人身份信息，数据的来源是世界商业信息服务公司巨头邓白氏（Dun&Bradstreet）。

泄露的数据中不仅包含普通公民的姓名、职称、职能、工作邮件、电话号码、工作单位的盈利情况，员工数量等信息，还包含了超过 10 万条的美国国防部的人员资料，其中有各种职务信息超过 1 万条，如职业军人，情报分析人员，弹药专家，化学工程师等。紧随其后的国家部门是美国邮政系统，有超过 88000 条员工记录，然后是美国陆军，空军和退伍军人事务部共计 76000 条左右记录。

（二） 英国移动运营商 Three 再曝客户数据泄露事件

2017 年，媒体报道的国外电信运行商的重大信息泄露事件并不多。其中，英国最大移动运营商 Three 的数据泄露风波最为引人关注。

2017 年 3 月，英国移动运营商 Three 客户数据再次被泄，这次是因技术问题导致客户的个人信息被泄。某些登录客户能查看其它用户的个人数据（姓名、地址和电话号码）和通话记录，但是未泄露任何财务数据。这并不是 Three 首次因数据泄露博得“头条”。2016 年 11 月，Three 证实遭遇大型网络安全事件，近 13.3 万用户的个人数据被泄。

（三） 枪支零售商气枪 GI 的论坛被黑客入侵；65,000 个用户帐户泄露

2017 年 2 月，黑客声称已经入侵了枪支零售商 Airsoft GI 的官方网络论坛，并在今天早些时候上传了 Dropbox 的数据。该论坛在 2017 年 1 月被黑客入侵，泄露数据首先被数据挖掘公司 Hacked-DB 发现，他们发现被盗的用户账户总数是 70,000，但经过深入的扫描发现 5000 个账户是重复的，被盗账户的确切数目是 65215。被盗的数据包括注册用户的个人信息，例如用户名，电子邮件账号，IP 地址和密码 bcrypt，Blowfish。在这些数据中，有 40,521 个 Gmail 账户，3,261 个雅虎账户，2,760 个 Outlook 和 2,760 个 Hotmail 账户。唯一 IP 地址总数为 17,364。

（四） 墨尔本国际射击俱乐部数据库被黑，超 1500 支枪械信息被泄露

2017 年 11 月，根据澳大利亚墨尔本警方的调查，有黑客在本月攻破了墨尔本国际射击俱乐部的数据库，其中包括超过 1500 支半自动手枪的信息记录，它们分属于 540 名俱乐部会员。数据具体记录了每位会员姓名、家庭住址、联系方式以及拥有的枪械数量、类型和存放地点。

警方担心的问题并不是数据库被黑这件事本身，而是这些枪械持有者的人生安全。因为这种案例很多，尤其是在农场和其他偏远地区，很多枪械持有者都遭遇过抢劫。更可怕的是，这些受害者往往是在射击俱乐部或其他地方进行过登记，相反，没有登记过的人反而很少会遭遇此类事件。

（五） 美国安全公司客户敏感文件泄露：多家财富 1000 强公司受影响

2017 年 8 月，信息安全公司 DirectDefense 发布博文声称在美国安全公司 Carbon Black 提供的端点检测和响应 (EDR) 解决方案中发现一个重大问题，后者泄露了客户数万份敏感文件。泄露的客户数据包括云密钥、应用商店密钥、凭证以及其它敏感商业机密。造成这种结果的原因是 Carbon Black 公司对第三方多频扫描器服务的依赖。

DirectDefense 公司声称，当这款工具在客户计算机上发现了之前从未见到过的新文件，就会首先将文件上传至 Carbon Black 服务器，然后将文件副本转发到谷歌的 VirusTotal 多频扫描服务来检测文件是否是恶意的。

（六） 犯罪分子花 40 多万元购买个人信息实施诈骗

2017 年 2 月 9 日晚，绍兴市公安局越城分局城南派出所接到公民虞某报案称，虞某当晚收到好友王某的一条信息，王某购买一件价值 1922 元的商品，因手机支付不成功，请虞某帮忙代付。虞某通过手机为好友支付货款后，对方再次要求付款，她疑心被骗因而报案。结果证明，王某的账号被盗，有人冒充王某对其好友实施诈骗。

警方在哈尔滨抓获这个利用社交软件冒充好友实施代付诈骗的犯罪团伙。在这个团伙的电脑中，绍兴警方发现大量公民个人信息。“信息最多的一台电脑中有 300 多 GB 的个人信息，包括多个邮箱、社交软件的账号和密码，而且都很准确。”据犯罪嫌疑人交代，这些信息是他以一组 2 元左右的价格，共花 40 多万元从吴某等人手中买来的。而吴某手中的信息则来自一个黑客犯罪团伙，该团伙利用超级 SQL 注入工具、网站漏洞扫描软件，批量扫描网站程序漏洞，非法获取网站后台用户注册数据。

（七） 工控安全事件：6000 多台 Lantronix 设备密码已经泄露

2017 年 12 月美国 NewSky Security 安全公司近期发现 6460 多台装备了 Lantronix 公司生产的网络设备发生了 Telnet 密码被泄露的事故。根据安全研究人员分析，如果这些 Telnet 密码被攻击者得到，他们就可以借此针对连接的设备发动大规模网络攻击。

另外，研究人员在 Metasploit 渗透测试论坛上发现了一个 Lantronix 的“Telnet 密码恢复”模块，该模块可以通过配置端口 (30718/udp，默认在 Lantronix 设备的旧版本上启用)，检索从 Lantronix 串口到以太网设备所记录的全部安装设置，并以明文方式提取 Telnet 密码。经过分析，此次问题就出在这些老旧设备无法更新并运行新发布的升级补丁。

第四章 关于信息数据保护的 policy、法规与技术

本章主要分析 2017 年国内外针对信息泄露问题出台的一些政策、法规，以及市场上出现的一些典型保护数据安全的技术案例。

一、 中国《网络安全法》规范数据保护，并对信息泄露事件追责

近几年，中国非常重视网络数据的保护，并出台了相关法规，对非法泄露数据、危害数据安全的行为予以严惩。事实上 2012 年 12 月全国人大就出台《关于加强网络信息保护的決定》。2017 年 6 月 1 日正式实施的《网络安全法》，专门列出了“第四章 网络信息安全”，对政企机构收集、使用和保护个人信息，防止信息泄露提出了一系列的要求。

根据网络安全法第四十二条规定：

网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

也就是说，保护系统中存储的个人信息，是网络运营者的法定义务。如果网络运营者因运维不利而造成个人信息泄露的，必须承担法律责任。

除了运营者责任角度，《网络安全法》第 27 条还从威慑不法分子角度规定，任何个人不得从事非法侵入他人网络、窃取网络数据等危害网络安全的活动。

另外，从促进安全技术创新角度，《网络安全法》第 18 条规定国家鼓励开发网络安全保护和利用技术，促进公共数据资源开放。

因此，从我国相关法律政策可以看出，遏制信息泄露，至少需要规范运营者义务、打击危害数据安全的不法分子，以及促进数据保护的技术开发与利用。

二、 国外政府对信息泄露事件处置的新法规

下面我们再来介绍两个国外政府在 2017 年颁布的，与防止信息泄露相关法律法规。相关信息介绍主要来自网络媒体。

（一） 澳大利亚着手出台《数据泄露通报制度》

2017 年 3 月，澳大利亚的 2017 年隐私权修正（数据泄露通报）法案标志着信息安全立法的一大里程碑。同时，澳大利亚正着手出台《数据泄露通报制度》，以尽可能的减少数据泄露事件给公民和机构带来的不利影响。

截至目前，包括澳大利亚在内的全球约 90 个国家已出台了信息安全相关法律法规，而其严格程度、执行方式以及处罚力度亦各不相同。目前美国约 47 个州拥有自己的安全违规通报法，尽管尚未在国家层面引入统一的法律要求。但大多数数据泄露事件仍然未被及时发现与报告。

（二）新加坡立法严格限制企业使用国民身份证权限，以防个人信息盗窃

11月8日消息，新加坡个人数据保护委员会（PDPC）正在修订国家“个人数据保护法案”（PDPA）指导方针，意在严格限制企业使用国民身份证（NRIC）权限，以防各组织或个人信息被用于盗窃、欺诈等非法活动。与此同时，该国还提出一项新安全法案，希望能够削减官僚作风、缓解各政府公共部门的数据共享问题。

知情人士透露，新加坡国家管理人员将于新法案正式通过后敦促所有公共机构与部委统一遵守规则，并授权公务员进行集体指导与监督。另外，新法案不仅要求政府机构只能在“数据共享法案”允许范围内共享数据，还制定了公民安全保障措施，以防任何数据遭到滥用。例如，在没有国家政府指示的情况下访问或披露用户数据，或将被判处高达5000新元的罚款或最高两年的监禁。

三、 快递行业对于隐私面单的探索实践

“隐私面单”是2017年国内快递企业开始尝试使用的一种新型用户个人信息保护技术。

所谓的“隐私面单”，是指面单上并不完整显示收件人的信息，而是通过技术手段将用户的手机号、姓名和地址等信息做加密处理，快递员通过公司自主研发的APP，直接拨号联系到收件用户，从而尽可能的保护用户的个人信息不在快递寄送过程中被非法窃取。

2016年末，京东就已开始试行“微笑面单”，包裹生成时用技术手段部分隐藏用户的姓名（只显示姓）和手机号（中间四位隐藏）信息，以萌萌的笑脸代替，以达到保护用户隐私的作用。



2017年年初，圆通速递在国家邮政局发展研究中心指导下率先研发推出“隐形面单”，客户可根据需求自由选择是否使用该项服务，但仅限于电子面单用户。

2017年5月，顺丰开始试点丰密运单。阿里旗下物流数据平台菜鸟网络，也于2017年

5月中旬联手 EMS、百世快递、中通快递、申通快递等，共同推动使用“隐私面单”，将面单上用户电话号码的中间四位用符号*代替。



不过，有媒体记者调研发现，隐私面单目前的使用占比并不高。相对来说，顺丰快递的隐私面单数量较多，不过占比也没有超过一半。总体而言，国内隐私面单的普及率仅 20%。

造成隐私面单使用率不高的主要原因有两个方面：一是很多普通用户还不知道快递公司可以提供这样的服务；二是隐私面单对于某些用户群体来说，使用起来还是不太方便。不过，这一积极的尝试，对于电子商务和物流产业高度发达的中国来说，还是非常有益的一步。