推动信息安全是企业的责任

罗立凡

Promoting Information Security Is the Responsibility of the Enterprise

Kevin Luo

信息技术特别是互联网在全球范围的迅猛发展，让我们生活的环境发生了革命性的变化，我们今天的衣食住行等一切行为，无不与信息、互联网密切相关，信息正像水、空气一样，成为我们生活中不可或缺的资源 . 事实上，现在以及未来，新一代的信息技术远远超过了我们现在感受到的力量 .

当我们每个人的每一次信息获取、每次购物、每次出行、每次思想交流等等这一切，都通过身边的信息终端汇聚成海量的数据时，当全球所有的人都通过信息终端进行与生命和生活相关的行为时，我们面临的是一个真正信息爆炸的时代，而这些大数据以及与我们相关和不相关的各种信息终端互联互通的数据，未来会重构我们的世界 .

这一切才刚刚开始 .

万物互联或者说物联网和下一代互联网的到来，不仅将使得云计算和大数据处理真正产生超过我们想象的价值，而且将催生出全新的商业模式甚至推动我们社会意识的重构 . 在这个过程中，第 4 次工业革命（工业 4.0）将在信息技术对整体社会生产形式的彻底改造中释放出巨大的能量 .

在不远的未来，全球的互联网用户、设备数量将以前所未有的速度增长，在线和移动应用的普及渗透将带动多元异构数据流量实现爆炸性增长 . 与此同时，在信息流的驱动下，物流、资金流在虚拟网络时空维度上高速交易流通，极大促进了全球贸易的发展和经济融合，各个国家在发展进程中你中有我，我中有你，更加紧密地联系在一起 .

我们面临的是一个具有无限可能又很难预测的未来 .

信息技术从诞生之初，就面临着安全和发展这 2 个命题，也可以说，它们构成了信息的两翼 . 在信息高速发展的现在以及未来，信息安全仍然是与信息迅速发展相生的另外一个核心 .

如何构建在云计算、物联网、大数据以及人工智能时代的泛互联网信息安全体系，确实决定了我们未来如何不被大数据和信息所吞噬 .

信息安全定义

由于信息以及互联网与我们的关系日益紧密，同时各种新的技术和商业模式的涌现，我们现在面临的信息安全成为了一个动态变化的概念，这其中有广义的信息安全成分，同时也混合着许多变化了的狭义信息安全的成分 .

事实上，信息安全的概念在20世纪经过了一个漫长的历史阶段，进入21世纪后，随着信息技术的不断发展，信息安全的问题也日显突出，更为广大公众所关注 .

国际标准化组织所定义的信息安全的含义，主要指的是信息的完整性、可用性、保密性和可靠性，这是基于对信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性基本特征所进行的一种规范 . 而事实上，信息安全的实质却是要保护信息系统或信息网络中的信息资

源免受各种类型的威胁、干扰和破坏，即保证信息的安全性．从这个意义上讲，信息安全不只是单纯的技术问题，而是将管理、技术、法律等问题相结合的体系．

从这些变化着的概念来看，信息安全的2个核心需要明确，即信息系统的安全和网络中的信息安全，这2个核心要点决定了现在以及未来信息安全的主要发展关键．

正是基于对信息系统的安全和网络中信息安全的认知，微软认为，信息安全对于公民（用户）、企业和政府3个主体拥有3种不同的价值和责任．

对于公民个人来说，信息安全意味着能够让个体感到安全，即所使用的信息环境可以保护其个人数据和隐私．

对于企业来说，网络安全意味着通过运维操作和信息安全操作，确保关键业务功能的可用性和保护机密数据．

对于政府来说，网络安全意味着要保护公民、关键基础设施和政府计算机系统免受攻击或威胁．虽然定义不尽相同，但是信息安全基本上代表聚合的活动和资源，以安全、专用和可靠的方式满足公民、企业和政府的计算目标．对于政府决策者来说，这类目标包括保护公共安全、经济安全和国家安全等．

如今，信息与网络通信技术是现代社会以及政府管理公共服务、确保经济增长和捍卫国家安全的重要基础．同样更重要的是信息与网络技术对其他行业的影响日益明显．先进的信息技术是帮助政府完成包括经济稳定与安全、社会稳定与自由、公共安全与教育的重要手段，也是催生新的商业模式和新工业变革的主要驱动力量．

但是，对信息与网络技术的依赖本身会带来不断变化的风险．从国家到高度复杂且资金充足的犯罪组织，再到联系松散的“黑客行动主义者”团体，都花费精力在利用和攻击重要性与日俱增的网络空间中．随着新环境和威胁不断出现，信息安全也必须随之不断提高．

所以政府、行业和企业必须合作开发相应的网络安全框架并不断致力于启发创新，使网络安全解决方案与动态的威胁环境保持同步．跟上不断变化的网络威胁环境的一个重要方法就是，确保政府和行业除了关注提供结果的过程外，也能够关注以结果为导向的结果．

2017年6月，中国《网络安全法》将正式实施，这是中国网络治理从量变到质变的里程碑事件，也是依法治国、依法治网进程的标志性事件，有利于在网络空间和通过网络空间实现国家治理体系和治理能力的现代化，全面提升网络强国建设的速度和质量．《网络安全法》主要明确了等级保护制度、关键信息基础设施保护制度、国家安全审查制度、数据离境存储制度、用户信息保护制度、安全认证和检测制度、监测预警和信息通报制度以及应急处置制度“8项制度”．

在这部法律里，中国第1次将公众（用户）、网络运营者（企业）及政府机构的信息安全责任和义务作了明确的界定，这也使得中国信息技术在高速发展过程得到了强有力的保证．

信息安全，微软使命使然

从计算机诞生起，安全就成为一种信息发展的共生体，同样，自计算机有了操作系统，微软就成了信息系统安全的第1批守卫者．对于微软来说，保护用户的信息安全是一种天生的使命．

目前，微软有机会服务全球数十亿计的网络信息系统用户，已经不能只思考技术如何让微软的收入最大化，而是更多地考虑自身的社会责任和企业使命，积极主动、务实地理解、关照、响应用户重要的利益诉求或困扰．

由于信息流动的全球性和跨地域等基本特征，我们面临的信息安全日益复杂．个人、商业组织、政府和公共机构在享受技术创新带来的巨大红利的同时，也面对日益复杂的网络与信息安全环境，以及来自公共健康和安全、经济安全、国家安全、商业安全和个人信息安全等领域的挑战，这也是当代数字化国家治理和数字化经济转型的关键所在．

据国家互联网应急中心（CNCERT）发布的《2014年我国互联网网络安全态势报告》显

示，仅2014年，中国就有多家知名电商、快递公司、招聘网站、考试报名网站等发生数据泄露事件；2014年5月，某知名手机厂商论坛数据泄露，由于用户管理模块存在漏洞，导致包括账号、密码和社交账号等800万用户个人信息泄露．而在《2015年我国互联网网络安全态势综述》中显示，2015年，我国同样发生了约10万条应届高考考生信息泄露事件、某票务系统近600万用户信息泄露事件等等．

据统计，到2014年恶意网络攻击给企业带来每年高达3万亿美元的损失．麦肯锡在世界经济论坛2014高峰论坛上发表的报告表明，虽然互联网经济创造了巨大的价值，但是网络犯罪造成的损失高达15%～20%. 根据美国非营利性组织——开放安全基金会和威胁情报咨询公司RBS——合作发布的报告显示，2013年，超过8亿条个人记录遭到泄露；2014年，这一数字更是增加了78%.

信息安全威胁已经不仅仅是特定地理区域内的个人、机构面临的特殊挑战．随着信息网络技术的快速普及和渗透，原先相对封闭的信息孤岛和边界被逐渐打破，个人隐私、重要商业数据，不可避免地暴露在网络空间的各种安全威胁下，中国也同样面临与全球其他国家地区相同的网络与信息安全的挑战．

微软正是秉承自己的使命，继续开拓信息安全的创新之路．在提高安全性、隐私可靠性和透明性方面，将继续加强与政府、企业和公民的合作，在联系更加紧密的社会中创造更安全、更值得信赖的计算体验．

多年来，微软在应对网络威胁，保障信息安全方面被视为行业典范和标杆．微软长期高强度地投入巨量的人力物力保障信息安全，在理念和技术上不断创新．同时，微软积累了数十亿客户管理信息安全风险的经验，这些经验使微软可以深入了解并预估当前和未来的种种挑战．微软在产品和技术发展的重大战略规划过程中，始终关注网络与信息安全，特别致力于开发和提供安全优质的产品和服务．微软与政府、行业机构和生态系统伙伴等重要利益相关方一起协作，致力于打造和维护良好的网络与信息安全环境，保护用户免受信息安全风险的威胁．

信息安全是一种责任

我们身处在一个信息包围的社会，正如前面所说，信息给我们个人、企业和政府机构都带来了巨大的便利和机会，同样，就信息安全而言，微软认为，信息安全，无论是对公民个人、企业还是政府机构，都是一项共同的责任．

事实上，从即将要实施的中国《网络安全法》来看，对个人而言，“国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境”；对于企业而言，“网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”；而《网络安全法》的制定和颁布，已经体现了国家对信息安全负责任的态度，同时也明确了相关责任，“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护．”

所以，保护信息安全是全社会的责任．

简言之，对于公众而言，需要合理合规模地使用信息系统和信息资源，才可能保证信息安全和个人隐私信息的有效性；对于信息运营者或信息系统提供者而言，需要保证系统的安全性和运行的稳定性，这是信息运营及系统提供者的基本责任；对于国家机构而言，构建信息安全体系，并通过法律手段打击危害信息安全的行为，才能保证整体社会信息的安全运行．

正是基于对信息安全是信息系统提供者和运营者的基本责任的认识，微软作为众多信息系统的提供者，从开发安全、数据安全、物理安全、运维安全、数据主权、隐私管控、服务可靠、透明保证等多方面构建了一套360度信息安全保障

体系 .

微软在总结数十年软件安全开发经验的基础上，在业界率先提出并应用了安全开发生命周期（securitydevelopment lifecycle,SDL）的理念和工具 . 这种理念是一种软件开发安全保障流程，包括7个阶段的安全做法：培训、要求、设计、实施、验证、发布和应急响应 . 安全开发生命周期理念从最原始的产品概念设计起，涵盖后续开发的全过程，严格遵照威胁建模、风险分析、安全设计、缓解和补偿控制、安全代码审核、安全静态测试、安全动态测试的流程，使用多样工具和步骤，最大程度地减少产品安全漏洞 . 从而确保产品在发布上市前孕育健康“基因”和“抗体”，提高产品设计的安全性，更好地应对无处不在的网络威胁 . 微软率先提出的安全开发生命周期的理念已被许多领先的软件或 IT 公司采纳和应用 .

在 SDL 应用基础上，微软在 Azure 智能云计算平台的开发和运维过程中，开展了“红蓝”对抗，模拟黑客入侵等常态化攻防演练，从实战的角度发掘产品和运维流程中的安全漏洞，并进行针对性的改进 . 在漏洞发掘的方法和工具上，微软已经遥遥领先于行业标准 .

同样，正是基于信息安全是微软服务的基本责任的认识，微软在保护用户信息和保护隐私方面，已经成为能满足全球不同国家要求的企业 .

微软在产品设计中充分考虑各国对于用户信息安全和隐私的相关要求，在全球范围内积极地进行有关用户信息安全和隐私方面的合规认证，从而实现最大限度地保护数据安全和用户信息安全和隐私的目的 . 例如，微软 Azure 成为首个遵循 ISO 27018标准认证的云计算平台，而 ISO 27018则是首个国际化云端隐私数据保护标准 .

2014年，经欧盟负责数据保护的权威机构确认，微软的企业级云服务完全满足欧盟隐私法律的高标准要求 . 这意味着存储在微软企业云上的个人数据，无论其在地理上存储在什么位置，都将成为欧洲极为严格的隐私标准的保护对象 . 客户可以放心地使用微软的服务，安全地通过微软云将他们的数据从欧洲传递到世界其他地方 . 微软成为第1个、也是目前唯一获得此项批准的公司 . 这项批准涵盖了微软的企业级云服务，包括 Microsoft Azure，Office 365，Microsoft Dynamics 365，Microsoft Intune.

信息安全是一种合作

信息化和工业化的广泛渗透和融合，不仅提高了整体社会信息价值，也让信息技术变成了各行各业所依赖的基础 . 同时行业的变化和服务的进化，也让信息成为我们每个人生存的一种基础性资源 . 这一趋势的不断发展，也让信息成为像水、空气一样流动于各种系统的信息流，这种信息的形态，让各信息平台既相互依存又相互制约 .

对于我们今天的信息社会而言，不仅全球有几十亿的用户和终端，同时也存在难以计数的信息提供者和运营者，它们之间形成了相对服务和被服务的关系，而这种关系，让信息安全成为一种建立在信息流基础上的合作形态 .

作为基础信息系统和平台的提供商，微软认为，基于信息的广泛性和全球性，信息安全必然是一种全球合作的形态 . 在这个动态的信息环境中，即有企业与政府之间的合作，也有企业与企业之间的合作，要建立可信计算平台和安全的信息平台，合作是一切信息安全的基础，就目前信息技术的发展而言，不可能会有一家企业或一个机构能独立完成信息安全的服务 .

为了推动信息发展及信息安全，微软于2003年发起了“政府安全计划（GSP）”，目的在于建立各国政府对微软产品安全性的信任 . 2016年9月，在中国国家互联网信息办公室的指导下，微软在北京设立的“微软技术透明中心”正式启用，这是微软“政府安全计划”的一部分 .“微软技术透明中心”启用后，中国信息安全测评中心（CNITSEC）和其他政府授权的机构将能够运用测评工具查看并分析微软的源代码，就安全优先事项开展技术讨论，这能够让大家切实感受到微软产品和服务的透明性、可靠性和安全性 . 而微软与中国政府基于信息安全的合作，正在推动着中国信息安全向国际水平前进 .

微软认为，“可信任的技术与安全是我们迈向第4次工业革命的基础 .”而这一认知和行动，

也为中国“2025中国制造”提供强有力的支撑.

同时在信息安全领域，微软的“反数字犯罪实验室”(Digital Crimes Unit)将积极与国家互联网安全应急响应中心和网络安全执法部门协作，一旦发现恶意网络安全违法行为，共同在全球范围内维护网络空间安全.

在企业合作方面，一方面微软通过其信息产品（Windows，Office等）和微软Azure可信云平台将信息安全传递到全球数十亿用户，也传递到通过这些系统、平台构建信息系统的企业；另一方面，微软广泛地与中国企业展开信息安全方面的合作，共同构建基于信息安全的各种行业性平台，为促进中国信息安全在各行业的推广努力.

信息的跨平台、跨区域传输特征，决定了信息安全提高需要信息传输过程中的各节点的共同努力，而这种努力正是信息安全领域的一种合作的基本特征，而这种合作的深入，将决定未来信息技术的发展速度.

信息安全是一种基础服务

信息已经成为人类社会的一种重要资源，而这种资源不仅成为社会发展、技术进步的推动力，也成为了人类生活必须的要素.

可以说，就目前的社会进步而言，我们已经无法离开信息，信息的存在正如同水和空气一样，成为我们时时都需要的必备品.

同样，正如如何保证水资源、空气质量一样，信息安全的重要性已经成为保证社会稳定和人类生活水平的重要议题.

从这个意义上讲，我们无法离开信息，就意味着信息安全已经成为一种人类社会的基础性服务，如同水电气风、交通等社会公众服务一样，虽然对于每个公众而言，我们可能无法实实在在的去感受它的存在，但我们却无法离开它而享受信息带给我们的便捷和价值.

随着云计算、大数据、物联网和人工智能的发展，由人类信息构成的数据将成为有类似货币性质的虚拟财富，信息安全将变得更为重要和不可或缺.

正是基于人类社会对未来信息技术和数字革命的预期，微软提出的微软三大社会使命——重塑生产力和业务流程、构建智能云平台、创造更个性化的计算.在这些信息系统和可信云平台中，信息安全从设计、安全与隐私、管控与合规、透明和可靠性等维度入手，系统性构建新型安全理念和技术框架，跨越全拥有寿命周期，保障产品和服务的网络信息安全.

而微软在赋能于社会的过程中，这种基于可信计算信念的确立，不仅将通过其服务影响数十亿用户对信息安全的认识和保护他们的信息安全，而且通过这种理念的传递，带动更多的企业，建立更多基于信息安全的技术和信息平台，进而推动全球新一代信息技术的发展和第4次工业革命的进程.

罗立凡

博士，毕业于北京清华大学并获得电子工程学士学位.罗博士同时拥有哥伦比亚大学电子工程硕士和博士学位和纽约Fordham大学法学院法学博士学位.罗博士现任微软公司助理法律总顾问、微软亚太研发集团法律事务总经理.负责微软（中国）网络安全相关的法律、法规、政策和合规，并全面负责微软亚太研发集团所有法律事务.微软亚太研发集团的总部在北京，是微软公司在微软美国总部以外最大的研发中心.此前，罗博士担任微软公司云计算和企业业务部门的知识产权总法律顾问及微软知识产权授权部门总监等.在1999年加入微软之前，罗博士在纽约的Pennie& Edmonds LLP律师事务所执业7年.