经济动态

第 59 期

经济运行部　　二〇一七年十二月二十九日

推进网络安全和信息化工作 向着网络强国扬帆远航

网信事业，代表新的生产力、新的发展方向。发展网信事业，全球竞相发力；建设网络强国，我们扬帆远航。各地各部门深入学习贯彻落实习近平总书记网络强国战略思想，开拓创新、砥砺奋进，信息化驱动引领经济社会发展作用凸显，群众在共享互联网发展成果上有了更多获得感，网络安全屏障不断巩固和加强，网络空间国际话语权和影响力明显提升，网信事业取得历史性变革和成就。

新高度：从“网络大国”到“网络强国”，互联网进入全新发展时期

“现在人类已经进入互联网时代这样一个历史阶段，这是一个世界潮流，而且这个互联网时代对人类的生活、生产、生产力的发展都具有很大的进步推动作用。”2012 年 12 月 7 日，党的十八大闭幕不到一个月，习近平总书记在深圳考察时作出这样的论断。

我国于 1994 年第一次全功能接入国际互联网。20 多年来，网民数量迅猛增长，规模超过 7 亿；网络基础设施建设成就斐然，固定带宽已覆盖全国所有城市、乡镇和 95%的行政村，中国已成为名副其实的网络大国。

时代，犹如一个严苛的考官，把机遇与挑战同时摆在世人面前：如何在互联网迅猛发展的基础上实现核心技术新突破、谋求国际竞争新优势？如何正确把握安全与发展的关系，以安全保发展，以发展促安全？

如何在错综复杂的经济社会形势下让网络空间清朗起来，更好惠及民生？

2014 年 2 月，中央网络安全和信息化领导小组成立，习近平总书记担任组长。2 月 27 日，在中央网络安全和信息化领导小组第一次会议上，习近平总书记明确指出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。”

从“网络大国”到“网络强国”，中国互联网向全新发展目标迈进。

从出席世界互联网大会，为世界互联网治理贡献中国方案、中国智慧，到主持召开网络安全和信息化工作座谈会，强调让互联网更好造福国家和人民，再到主持中共中央政治局第三十六次集体学习，强调以 6 个“加快”建设网络强国……习近平总书记一系列深刻精辟的论断，一整套着眼长远的布局，为网信事业发展提供了根本遵循，为网络强国建设指明了前进方向。

举旗定向，蓝图绘就，号角吹响。

——网信工作的“四梁八柱”基本建立。中央作出一系列关于网络安全、信息化发展、网络空间国际治理等方面的决策部署，出台一系列战略纲要、发展规划、指导意见，为网信事业的健康发展保驾护航。

——网信工作“一盘棋”格局基本形成。目前，中央、省、市三级网信管理工作体系初步建立，部分省市网信办向区县一级延伸，建立完善重大项目会商、重要事项和重大决策督办等机制。

——网络人才队伍富有朝气充满活力。我国实施网信领军人才、高端人才、青年专家、特殊人才选拔培养计划，授予 29 所高校网络空间安全一级学科博士授权点，创建国家网络安全人才与创新基地，加快网信高端智库建设，为网信工作提供强大的智力支撑。

“随时以举事，因资而立功，用万物之能而获利其上。”在以习近平同志为核心的党中央的坚强领导下，各地各部门主动适应和引领新一轮信息革命的浪潮，网信事业扬帆远航。

新动力：深入推进“互联网+”，数字经济成为经济增长亮点

面对信息革命的挑战，“拥抱时代”才能“发展中国”。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上指出：“我国经济发展进入新常态，新常态要有新动力，互联网在这方面可以有大作为。”

2017 年“天猫双 11”全球狂欢节成交额达到 1682 亿元，交易覆盖 225 个国家和地区，全球超 14 万个品牌的 1500 万种商品参与，其中，共有 167 个品牌商家成为“亿元俱乐部”成员，其中有 97 家品牌实现半日成交额过亿。

有业内人士评价，“单日成交过亿”既是品质消费的体现，也是中国经济提质增效的结果，更是互联网技术推动的商业蜕变。近年来，电商交易额飞速领跑，移动支付全球领先，共享经济世界瞩目……一大批具有创新活力的互联网企业纷纷涌现，阿里巴巴、腾讯、百度、华为等一批网信企业的国际影响力日益提升。2016 年，在全球互联网企业市值前 20 强中，我国企业占据了 7 席。

互联网不仅催生了新业态、新模式，还让众多传统产业再现生机活力。各行各业都在发挥信息化对全要素生产率的提升作用，推动互联网和实体经济深度融合。如今，许多生产车间俨然是大数据工厂，接收订单、安排生产、物流配送都是信息化处理，机器换人，精确高效。在浙江设立国家信息经济示范区，在天津等 12 个城市设立跨境电子商务综合试验区，在贵州、上海等地建设国家大数据综合试验区……我国的数字经济总量跃居全球第二，成为经济增长的亮点。

惟创新者进，惟创新者强，惟创新者胜。近年来，我国着眼抢占信息技术发展制高点，推进人工智能、云计算、大数据等前沿技术研究，加大对集成电路、基础软件、工控软件等领域投资，高性能计算、量子通信、5G 等取得重大突破，特别是中国“芯”超级计算机首获世界冠军、世界首颗量子科学实验卫星腾空而起……网信事业在经济社会发展中发挥着越来越重要的作用，信息技术也正从“跟跑并跑”向“并跑领跑”转变。

新生活：亿万人民在共享互联网发展成果上有更多获得感

习近平总书记指出：“必须贯彻以人民为中心的发展思想”“让亿万人民在共享互联网发展成果上有更多获得感”。

为发挥互联网在助推脱贫攻坚中的作用，推进精准扶贫、精准脱贫，让更多困难群众用上互联网，2016 年 10 月，中央网信办、国家发展改革委、国务院扶贫办联合印发《网络扶贫行动计划》，提出实施“网络覆盖工程、农村电商工程、网络扶智工程、信息服务工程、网络公益工程”五大工程。“淘宝村”帮助特色农产品从大山深处走向全国各地，

“远程教育”让山沟里的孩子可以接触到名校名师，“网络分级诊疗”打通省、县、乡三级医生资源合作体系……脱贫攻坚事业更广泛、深入地插上“互联网+”的翅膀，得以更强劲、更迅捷地推进。

为适应人民期待和需求，加快信息化服务普及，降低应用成本，为老百姓提供用得上、用得起、用得好的信息服务，近年来，在宽带中国等战略指引下，一条条信息“高速路”在中国版图上迅速铺开，一个个信息孤岛加快消除，即使是偏远地区，光纤宽带入户、优质网络也越来越普及。与此同时，手机国内长途和漫游费正在取消、国际长途降费已提上日程，中小企业互联网专线接入资费明显减少……

为加快推进电子政务，鼓励各级政府部门打破信息壁垒、提升服务效率，让百姓少跑腿、信息多跑路，解决办事难、办事慢、办事繁等问题，近年来，各地着力打破数据孤岛，加强信息共享，变“群众来回跑”为“部门协同办”，与民生相关的各个领域都在触“网”中。轻点鼠标，就可以实现下单、付款，喜爱的商品可以直送到家；动动指头，就可以在网上办理业务，不用再跑多个部门排几个小时的队了……

为让互联网成为党委政府与群众交流沟通的新平台，成为了解群众、贴近群众、为群众排忧解难的新途径，成为发扬人民民主、接受人民监督的新渠道，目前很多地方和部门开设了网页、微博、微信、移动终端等，及时了解群众所思所愿，广泛征求意见建议，主流媒体积极推进传播手段建设和创新，传递正能量，唱响主旋律，构筑网上网下“同心圆”。

新气象：网络生态进一步好转，网络空间清朗起来

互联网为人们带来便利的同时，也伴随着不少隐患：一组代码、一条短信、一个电话、一页链接，可能导致个人财产蒙受损失、公共设施遭受侵犯。如今，网络已被视为继陆地、海洋、天空、外空之外的第五空间，“没有网络安全就没有国家安全”。

安全是发展的前提，发展是安全的保障。党的十八大以来，我国始终坚持依法治理、依规治理、依标治理，多措并举，多管齐下，多方参与，互联网治理模式和治理能力的现代化水平不断提升，网络生态进一步好转，网络空间清朗起来。

——网络立法进程加快。制定出台《网络安全法》这一网信领域基础性法律，推动《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》等出台，使现行法律延伸适用于网络空间。同时，建立关键信息基础设施保护制度，完善网络安全等级保护制度，出台“微信十条”“账号十条”“约谈十条”等管理规定，为依法管网、办网、用网提供了基本依据。

——从严整治网络乱象。近年来，国家网信办与多部门联动，动员社会各方力量，开展了一系列治理行动，比如持续整治网络谣言、打击暴恐音视频、打击网络色情、打击“伪基站”，清除网络敲诈和有偿删帖乱象……

——网警执法常态化。据统计，我国网络犯罪已占犯罪总数的 1/3，并以每年 30%以上速度增长。公安机关适应新形势，拥抱新技术，主动开展网上警察执法，全面提高网上见警率、管事率。目前 371 个省市公

安机关开通网警巡查执法账号，在重点互联网服务企业和单位建立网安警务室 1116 家。

网络安全为人民，网络安全靠人民，各类宣传教育活动深入开展，网络安全防线不断筑牢。手机连上一个免费无线密码，你的访问网站、聊天记录统统都被截取；当你穿过一道特别的安检门，将钱包放在传送带的塑料筐中，身份证号、银行账户信息实时显示在后台屏幕上……自 2014 年起，我国连续举办国家网络安全宣传周，提醒广大群众防范身边的网络安全风险。

新格局：携手共建网络空间命运共同体

2014 年以来，由我国倡导的世界互联网大会已经连续举办三届，旨在搭建中国与世界互联互通的国际平台和国际互联网共享共治的中国平台。习近平总书记指出，“互联网让世界变成了地球村，推动国际社会越来越成为你中有我、我中有你的命运共同体。”“互联网发展是无国界、无边界的，利用好、发展好、治理好互联网必须深化网络空间国际合作，携手构建网络空间命运共同体。”

近年来，我国始终以和平发展、合作共赢为主题，以构建网络空间命运共同体为目标，就推动网络空间国际交流合作提出中国主张，为破解全球网络治理难题贡献中国方案。

深化国际合作。2016 年二十国集团杭州峰会制定了《二十国集团数字经济发展与合作倡议》，“数字经济”成为盛会热词；“一带一路”建设信息化发展进一步推进，统筹规划海底光缆和跨境陆地光缆建设，提高国际互联互通水平，打造网上丝绸之路。伴随着国际合作的不断深

化，我国互联网企业的品牌逐步拥有了世界级的影响力，以 BAT 为代表的互联网企业正在通过搜索、电商、即时通信等产品输出中国影响力，和全球主流科技企业展开对话。第三十九次《中国互联网络发展状况统计报告》显示，截至 2016 年 12 月底，我国境内外互联网上市企业数量达到 91 家，总体市值为 5.4 万亿元人民币。

参与国际规则制定。2017 年 1 月，中央网信办、国家标准委牵头建立了国家信息化领域标准化工作统筹推进机制，加快推动中国信息化标准走出去。在云计算、大数据、物联网、智能制造、智慧城市、网络安全等关键技术和重要领域，我国积极参与国际标准制定。2017 年 3 月 1 日，我国发布《网络空间国际合作战略》，指出国际社会应携起手来，加强对话交流，共同维护网络空间和平、稳定与繁荣，共同构建网络空间命运共同体。

只有建立互联网新秩序，建立共同遵守的公约，才能保障互联网安全、健康、有序发展。国际舆论积极评价，“构建网络空间命运共同体”的主张，反映了国际社会的共同心声，为推进全球互联网治理贡献了中国智慧。

当今世界，信息技术革命日新月异；当代中国，网信事业发展大潮涌起。在习近平新时代中国特色社会主义思想的指引下，中国必将以更自信、更有力、更坚定的步伐，不断开创网信事业发展新局面。

————〈全文〉

恶意软件数量猛增 共建网络安全成全球共识

第四届世界互联网大会 12 月 3 日至 5 日在浙江乌镇召开。数字经济发展成为本届大会热门议题，各界人士表示，随着人工智能、物联网等新一代互联网技术应用，数字经济将得到长足发展，并成为全球经济发展的新动能。与此同时，业内人士担忧，随着互联网发展，网络安全威胁也与日俱增，从根本上解决这一问题需要全球携手共建网络安全。

日益凸显的网络安全威胁引起全球高度关注。卡巴斯基实验室创始人和主席尤金·卡巴斯基在大会期间介绍，1997 年卡巴斯基刚成立时一年共收集 500 个恶意软件，10 年后的 2007 年收集了 200 万个恶意软件。2017 年，卡巴斯基预计将收集到 9000 万个新的恶意软件样品。恶意软件数量增速之快，从一个侧面反映出网络安全形势日益严峻。

360 集团创始人兼 CEO 周鸿祎表示，未来网络安全与各国命运与共、休戚相关，网络安全的新威胁、大挑战，会成为国家安全和发展的潜在威胁和阻力。尤其是互联网金融、物联网大力发展的今天，网络安全威胁不仅仅威胁到信息安全，更会威胁经济安全、社会安全、城市安全乃至国家安全。他认为，应对网络安全威胁，要推动建立网络安全信息共享机制，建立常态化的应急响应机制。同时，企业与企业之间、企业与政府机构之间，应该建立大合作，一起应对未来的网络安全问题。

尤金·卡巴斯基则表示，网络病毒是跨国的，而且非常国际化。随着世界数字经济发展，网络安全威胁不断增加，各国应加快进行网络安

全建设。他建议各国联合起来共同应对网络安全威胁，共建全球网络安全体系。

目前，我国对网络安全形势高度重视，政府机构和企业已开始联手建立相应的安全防范机制和体系。如工信部公布了《公共互联网网络安全突发事件应急预案》，明确了相关的防范和应急措施。12 月 4 日，中国信息通信研究院泰尔终端实验室、360、华为、vivo 等多方成立移动安全联盟，力求联合各界力量共建网络安全产业链。

————〈全文〉

中国企业网络安全投入高于全球平均水平

7 日，普华永道发布全球信息安全状况调查（以下简称调查）显示，中国内地与香港企业在网络安全方面的平均投入比全球数值高出 23.5%，受访企业的平均预算达 630 万美元。

83%的中国受访企业表示，数字化转型是促使其投资网络安全的重要契机。在具体的投资布局上，64％的受访企业将物联网安全（IoT）标记为最优先项，60％的受访者看重企业业务、数字化与 IT 三部分的融合，而生物识别技术和高级认证机制则位列第三，得到 57％受访者的认同。

普华永道中国网络安全与隐私服务合伙人李睿表示：“调查发现，在中国的许多企业尤其是技术为上的企业，对于网络安全的潜在威胁反

应越来越敏捷，因为他们有很强的网络安全保护意识，期望先发制人，防范风险。”

调查认为，随着科技飞速发展，人工智能、物联网、RPA/IPA、区块链、大数据分析、云以及增强现实/虚拟现实等一系列新技术正进一步颠覆全球商业格局。中国在物联网发展和应用上处于世界领先地位，随之而来的冲击也日益凸显，因此企业在应对相应威胁时也较为积极。调查数据显示，72%的中国内地与香港受访企业对此有积极回应，表示其针对物联网安全的战略已经就位，这一数值高于全球水平。

近期发生的多起网络安全事件表明，网络安全不仅会干扰商业的正常运营，也会引发对整个商业环境安全的担忧。根据调查反馈，中国内地与香港有 46%受访者表示客户数据泄露是最直接影响，而财务损失（38%）和商业邮件入侵（36%）紧随其后。

同时，由于智能设备在工作场所中的普及，46%的中国内地与香港受访企业将移动设备列为信息安全事件的攻击目标，攻击来源主要指向离任前雇员与竞争对手，二者比率十分接近，分别为 42%和 41%。

调查还表明，在当前复杂多变的网络安全大环境中，首席信息安全官（CISO）与首席安全官（CSO）在中国企业中的重要性开始突显，同时专业安全管理职位也相应增多，尤其是在以科技为主导的企业中。有50%的中国受访企业表示，他们的首席信息安全官或首席安全官均直接向首席执行官汇报。

普华永道中国网络安全与隐私服务合伙人冼嘉乐表示：“企业面临的安全性挑战复杂多样，无论是立足中国市场求发展，还是希望进军海

外市场，我们建议企业积极顺应技术发展，以更好地挖掘其商业潜力，修复信息安全方面的短板。展望未来，明智的安全策略将有效降低网络安全的威胁与风险，同时也会助力企业在日趋严格的全球信息安全监管环境中保持正确的方向。”

————〈全文〉

网安新规实施 各企业强化信息安全管理

去年 11 月 7 日，中国首部《网络安全法》获全国人大常委会表决通过，于 2017 年 6 月 1 日起施行。随着互联网发展的持续深入，网络成为企业基础设施的一部分，网络安全也成为国家安全的一部分，对关键信息基础设施而言更是“国之重器”。而国内在网络安全信息建设方面缺口极大，该法的颁布也是意料之中。据统计，在新技术和大数据快速变化的环境之中，中国网民每年的经济损失是 916 元（中国网民数量为 9 亿）；中国的防范网络犯罪的专业人才缺口是 140 万（目前仅 3 万）；中国有信息安全相关责任和义务的企业法人有 5 万家。而《网络安全法》从 2013 年下半年提上日程到 2016 年年底颁布，论证、起草、出台，速度非常快，充分说明了出台这部法律的重要性和紧迫性。

今年 5 月以来，大数据行业风声鹤唳。由于上游主管部门的重拳出击，15 家数据公司被列入调查名单，其中几家估值都超几十亿。据多位知情人透露，“数据堂”多人被警方调查，导致部分数据业务线停摆，

整个公司业务呈收缩状态。而被调查的原因，相关人士称是因为数据堂给一家理财营销公司提供了大量涉及用户隐私的数据。

整治行动的规模，超乎所有人的想象。多位业内人士预测，这轮清理行动恐怕只是一次预热行动，更大的风暴还在后面。而下游数据需求方也未能幸免，客户开发受到严重影响。

不过，《网络安全法》并未对泛滥流动的数据实现一刀切。“网络安全法里面有一条，指‘经过处理无法识别特定个人且不能复原的除外’，即匿名化后的信息不再属于个人信息。”中国信息安全研究院副院长左晓栋表示，这为大数据应用留下了充分的空间，应该鼓励更多地使用匿名化措施，既充分保护个人信息，也有利于大数据应用。《网络安全法》第三十七条规定关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。这与央行对银行业金融机构的监管思路不谋而合。上述规定会对境内银行业金融机构的现行操作造成的影响目前还有待观望。考虑到实践中外资金融机构确有与境外关联机构共享个人金融信息的需要，若需维持现有操作，境内银行业金融机构至少需要“按照国家网信部门会同国务院有关部门制定的办法”进行“安全评估”。

《网络安全法》颁布后，为有效增强员工对其深入了解，不少企业纷纷组织学习。上海浅橙网络科技有限公司特邀锦天城律师事务所高级合伙人吴卫明博士围绕《网络安全法》对公司全体员工进行了专题培训。谷安天下特推出《网络安全法》宣传教育解决方案，帮助各组织单位开展《网络安全法》的宣传教育落地工作。《网络安全法》实施一月后，

为了总结和推广中央企业网络安全综合解决方案的优秀成果，公安部网络安全保卫局等组织开展了“2017 中央企业优秀网络安全综合解决方案”申报评比活动。此次活动共收到 40 家中央企业和金融机构申报的 71 个方案。申报单位涵盖了能源电力、交通运输、建筑、通信、电子、航天军工、银行、保险等主要行业，申报方案涉及到网络安全、云计算、大数据、移动化、商密网等多个方面。

同时，各央企也打响信息安全保卫战。国药集团建立企业信息安全管理、运维、技术体系，并致力打造云安全下一代防御体系。中国中铁也深刻认识到传统信息安全体系的不足，主动谋划新的信息安全管理思路，采用新技术加固安全防线，并成立网络安全事件应急处置小组，由公司副总裁担任组长。另一方面，伴随《网络安全法》的提出，越来越多的企业开始意识到用户信息窃取、诱骗欺诈等恶意行为的影响和危害，对移动办公平台数据安全性和私有化的要求也越来越高。

————〈全文〉

企业网络安全靠两招：技术自主创新 加强制度建设

随着越来越多企业使用移动办公，以及物联网应用爆发式增长，企业所面临的网络信息安全风险成倍放大。但是，很多企业还没有意识到信息安全形势之严峻，防护力量普遍不足。必须“双管齐下”，一方面通过自主创新为企业安全防护提供更加可靠的技术支持；另一方面加强企业网络安全制度建设，从管理上堵住漏洞。

从 5 月份的“Wannacry”到 6 月份的“Petya”，勒索病毒今年的两次爆发给全球企业敲响了安全警钟。信息安全厂商奇虎 360 公司董事长周鸿祎坦言：“在一定程度上，这是对我国网络安全状况的一次小小压力测试。”中国工程院院士沈昌祥表示：“这也说明传统的封堵查杀被动式防御已经过时，企业的安全形势发生了巨大的变化。”

信息安全产业的迅猛发展也从侧面印证了企业网络安全形势严峻。来自市场研究机构前瞻产业研究院的数据显示，2016 年全球信息安全行业市场规模约为 2392.51 亿元，同比增长 19.16%。从 2006 年的 452.91 亿元发展到 2016 年的 2392.51 亿元，11 年间，市场规模增长了 5 倍；在我国，2016 年信息安全产业市场规模也达到了 477 亿元，未来 5 年预计将保持 10%以上的增长。是什么让企业面对的网络安全形势发生了前所未有的变化？新的安全锁又在哪里？

“万物互联”新考验

“从电脑端向移动端迁徙，包括企业员工开始大量使用包括手机在内的自有设备工作，给企业安全形势带来了巨大的改变。好比过去你只是守一个孤岛，比较容易，现在却打开了很多扇窗。”企业级移动工作平台蓝信商务总监李悦告诉记者。

的确，来自市场研究机构 IDC 一份调查显示，60%的企业员工会将商业机密数据储存在其智能手机中。2016 年，中国移动办公人数达 4.45 亿人，同比增长 13%；预计到 2018 年，移动办公人员数量将超过 6 亿。互联网安全厂商瑞星安全专家唐威表示，由于员工频繁使用智能手机等

个人办公设备连入外网，一方面病毒防御成为严重的安全隐患，另一方面手机也有可能成为信息泄露的出口。

在移动互联网普及后，“无处不在”的物联网又让网络安全形势变得更为复杂。中国移动通信集团信息安全与运行中心总经理张滨表示，有数据显示，到 2020 年全球连入物联网的设备将达 500 亿个，无论智能家居、智慧城市，还是智慧交通、智能制造，物联网应用将无所不在，这也让病毒攻击的后果更加严重。

亚信安全首席技术官张伟钦则在 C3 安全峰会上表示：“物联网设备的操作系统五花八门，且存在漏洞，有漏洞就会受到攻击。想象一下，如果有人控制了企业的摄像头，并以此窃密呢？这样的攻击会比我们想象中来得更快。”

不过，企业对安全形势的变化开始有所准备。市场研究机构 Gartner 的报告指出，尽管目前仅有 16%的企业应用网络安全产品来为其至少一款移动或者物联网关键应用提供防护，但有 26%的企业预计会在 2019 年之前使用应用保护产品。

技术创新增强“战斗力”

在国家保密局科技司司长刘艳看来，想要“魔高一尺道高一丈”，首先要技术创新，“通过自主创新来为企业安全防护提供更加可靠的技术支持”。

技术创新来自对实际情况的清晰把握。李悦表示，移动端泄密有多种情况，需要通过技术创新加以控制。“比如蓝信不仅能实现阅后即焚、转发限制等功能，甚至如果企业员工用手机截屏操作，后台也会有所记

录，知道是谁截屏了什么内容，文档阅读器也是内嵌的，可以给分发给每个人的工作文档加水印，同时不再需要调用第三方应用，这样就能有效保障工作文档不流出。”

技术创新也需要不断融入前沿技术成果。张滨表示，解决物联网的安全风险，态势感知是关键。“比如对基于物联网终端的业务数据、业务流量、外部情报信息，如果能及时发现异常行为，并及时处理，就能主动预防安全风险。”亚信网络安全产业技术研究院副院长童宁则告诉记者，安全厂商正试图将人工智能中的机器学习应用于态势感知，“机器学习可以将病毒攻击或者异常行为的特征抽取出来，并加以过滤，使判断更加快速准确，同时前端主动拦截的成功率也能大幅提高”。

不过，要想全方位应对威胁入侵，需要的不仅仅是技术。唐威表示：“一方面在技术上需要选择专业化更高、覆盖更全面的安全产品；另一方面也要在管理上建立严格和切实可行的机制。”

机制带来“长效化”

“企业的安全保障要靠技术，也要靠制度和管控。”沈昌祥说。在他看来，企业网络安全制度的建设，需要在分析风险的基础上，实行准确的等级划分。“从保护业务信息和系统服务两维资源出发，根据在国家安全、经济建设、社会生活中的重要程度，以及系统遭受破坏后的危害程度等因素来确定等级。比如，最高等级在顶层设计上，就需要以专门监督检查、实时监控实时处置为原则。”

Gartner 全球研究总监张毅则认为，企业网络安全制度建设还要从单纯的防御防护，逐渐迁徙到对整个流程的优化，“除了通过技术防护

之外，还需要重新梳理业务流程，来减少安全漏洞，比如各个业务部门的工作如何协调与整合”。

在思杰大中华区总裁曹衡康看来，企业网络安全制度的建设，还要重视人的因素。“比如企业制定从上到下的安全策略时，需要让尽可能多的部门员工、利益相关方提出意见和建议，同时要为所有员工提供必要的工具、指导和培训，以提升员工保护企业安全的主观能动性。通过提供认证、全面的课程培训以及免费的学习机会，提高员工识别潜在攻击并及时作出响应的能力。”

亚信安全董事长何政表示，各企业需要在网络安全防护上相互配合。“随着网络安全形势的变化，靠一家企业的力量很难应对挑战，必须齐抓共管，同时引入更多社会化服务提供安全保障。”

————〈全文〉