神舟电脑发布2015夏季新品

7月9日，神舟电脑在京发布2015夏季新品，围绕“我本轻薄”这一主题，神舟电脑发布多款全新产品。优雅XS-5Y10S1和XS-5Y71S1打破14英寸笔记本的记录，比macbook air系列中13.3英寸机型的17mm机身还要薄1mm，优雅XS系列以纯银白色打造，采用无风扇、零噪音设计。其配备的5200mah超大容量电池，连续播放高清视频可达8小时，最长待机时间高达一周，完全可以满足人们随时随地的娱乐需求。三款各具特色的PCpad升级版产品也同期亮相，屏幕尺寸从10.1英寸跨度到13.3英寸，融入英特尔酷睿M处理器、windows8.1操作系统、4G以上内存和128G以上的SSD硬盘等，性能强大实用。神舟PCpad平均厚度都在10mm左右，并全面升级至USB3.0接口，同时采用IDT技术，全面实现了有电源即可开机工作，告别了由于电池过放导致的长时间充电才可正常工作的电源解决方案。当外接搭配的皮套键盘时，轻松实现PC平板二合一。

此外，神舟推出的搭载台式机CPU和G-sync技术的战神GX8 PRO笔记本又一次走在了行业的前端，整体厚度仅有35.7mm，孤岛式的全彩背光键盘彰显华丽形象。双风扇七铜管保证散热完美，GTX980M的显卡搭配G-sync显示屏配合i7-4790K的处理器，2×256GB M.2的固态硬盘加上2TB的机械硬盘搭配32GB DDR3L的内存条，让整机性能得到了真正的王者体现。

（陈杰）

瑞星携江西民政造整体安保方案

日前，瑞星与江西省民政厅达成合作伙伴关系。瑞星将借助自身品牌实力和技术积淀，为江西民政“数字民政”移动应用平台打造一整套信息安全解决方案。该解决方案集结了瑞星高端系列防毒墙、网络安全预警系统和瑞星运维管理审计系统三项硬件产品以及国内首家虚拟化安全和终端安全管理等软件产品。

据了解，江西数字民政项目的安保项目主要分为移动应用平台和终端的安全防护体系两个部分。瑞星针对江西民政的实际需求，对移动业务应用层、网络层、终端接入层等三方面建立全面防病毒安全防护体系，保障服务器、计算机终端、网络设备等免遭病毒侵扰，建立起组织管理和技术支撑为一体的全网病毒预警、防范体系，将江西地区的民政服务质量和管理水平提升一个新的台阶。

（陈杰）

VERITAS发布更强性能的云备份产品NETBACKUP 7.7

Veritas公司7月9日宣布推出最新版本的企业级数据保护解决方案Veritas NetBackup 7.7。作为行业领先的解决方案，NetBackup 7.7将提供全新的强大功能，通过利用云存储服务极大提高备份和恢复的操作有效性，并向新兴的云服务提供商提供更多支持。NetBackup 7.7也进一步提升自身性能高达30倍。

“随着IT基础设施在云端投入的不断加大，大多数企业都将云存储作为备份存储的后继之选，以希望获得弹性、敏捷性，以及运营支出方面的优势，或仅仅是为了采取最新的磁盘备份技术。”Veritas公司大中华区总裁萧建生表示，“NetBackup 7.7将通过更优化的方式利用这些存储解决方案，帮助IT部门在丝毫不影响性能的前提下，轻松将云存储融合到备份战略中来。”

最新版本的NetBackup 7.7能够极大提升备份直转云存储服务的性能和互操作性，例如由Amazon Web Services（AWS）、Google、Hitachi Data Systems（HDS）、Verizon和Cloudian等提供的云存储服务。NetBackup 7.7还将提供突破性的集成功能，集成对象包括VMware vSphere Virtual Volumes、Microsoft Hyper-V、NetApp Clustered Data ONTAP（cDOT）以及Microsoft SQL Server等。此外，NetBackup 7.7将提供增强的自助服务功能，IT和非IT用户都可以通过直观的界面和本地工具，独立管理和控制备份与恢复活动。

“随着企业数据的数量和范围的不断激增，企业亟须更强大的工具来充分保护数据，以防丢失。NetBackup 7.7能够通过卓越的性能和高效存储技术，实现更快、更轻松的恢复，更有效地管理堆栈每一层的数据保护。”IDC存储系统和软件研究总监Phil Goodwin表示，“通过提高性能和扩大服务商选择，NetBackup 7.7的全新升级能够帮助企业获得云存储带来成本效益和运营敏捷性。”

（李炜）

打破网络安全神话 安全的关键是平衡

组织尝试解决网络安全风险的最大挑战之一，就是在网络安全开展工作中所面临的众多最基本的安全误区，这些误区常常导致组织对威胁的错误评估、资源的滥用，乃至不恰当安全目标的设定。消除这些误区，揭开网络安全的神秘面纱，打破网络安全的神话，是保证组织顺利开展复杂的信息安全工作的关键。

神话一：网络安全就是保护好数据

这是对网络安全最多的一种误读，认为所谓“网络安全”就是确保数据的访问安全，确保数据不被用于未经授权的目的，确保数据不被未经授权的用户使用。这虽然无疑是网络安全的一个关键问题，但数据所在的系统和网络还要必须防止攻击。例如，拒绝服务攻击（DoS）就不是为了获取企业的敏感数据，但它却能防止包括企业客户、合作伙伴在内的其他人访问和使用这些数据。

神话二：网络安全就是保护好隐私

另外一个对网络安全常见的误解就是，网络安全就是为了保护好个人身份信息。保护个人信息显然至关重要，但其他类型的信息也必须应该能够受到保护。这些其他类型的信息包括商业秘密及其他知识产权（如公司的软件产品源代码）、竞争信息（如客户和供应商列表）、定价和市场数据、公司财务信息等等。确保列入供应商和商业合作伙伴关系的所有形式的保密和专有信息受到保护尤为重要。

神话三：网络安全就是保护好机密

那么这么说，网络安全就是保护好机密，确保数据未被泄露了，比如，数据既没有被未经授权的用户使用，也没有被用于未经授权的目的？其实不然。因为真正的数据安全，必须确保其保密性，必须确保其完整性，必须确保其需要时的可用性，即信息安全圈著名的CIA原则。

C——“保密性”（Confidentiality）：指保护数据不受未经授权的访问，并且未被泄露。

I——“完整性”（Integrity）：指数据的准确性值得信赖，没有受到未经授权的变更。几年前，就有一家著名的黑客杂志刊登过一篇文章，指导那些觉得自己即将被解雇的员工如何给他们的雇主一点颜色看看。文章特别提到了几种方法，雇员不费吹灰之力就可以让公司的数据面目全非，如更改主要供应商的账户号码、更改发货地址等等。

A——“可用性”（Availability）：指在需要时数据可供访问和使用。只维护了数据的保密性和完整性，而当用户需要的时候，却无法访问和使用，那一切就等于零。例如，DoS攻击就是在不破坏数据的保密性和完整性的情况下，专门让系统和数据无法访问和使用的攻击手段。

神话四：黑客都是技术高手

这是企业专注于制定针对专业黑客的安全措施、防止具有高度熟练编程能力和技术的个人或实体进行攻击时最常见的一个错误。然而，这样的技能已经不再是黑客的先决条件。如今，即使没有什么技术知识的人也可以在网上找到简单易用而又能对企业带来巨大伤害的黑客工具。这样人在黑客社区有时被称作“脚本小子”，因为他们不需要真正的黑客知识。也有各种现成的书籍，可以快速培养新手关于黑客方面的技术。甚至有本畅销书竟然有一章叫《如何三十分钟成为一名黑客》。

最后，如今黑客使用的最有效的攻击手段之一社会工程攻击根本就不需要任何的技术能力。相反，做为一名高效的社会工程师，所需要的不过是自信和对人性的了解。社会工程攻击最普遍的形式之一就是钓鱼攻击，即黑客发送虚假邮件索取敏感信息，或在邮件中包含安装可影响公司网络恶意软件的附件。最近钓鱼攻击和其他社会工程技术进行协同在世界范围内攻击银行机构，造成了3亿美元乃至可能高达10亿美元的损失。

神话五：可以实现100%的安全

对网络安全最常见的认识误区之一还有就是可以实现绝对的安全，并且绝对安全是法律规定或行业惯例。这都是不对的。法律和行业惯例对企业的要求也都要合情合理。研究表明，即使规定企业将整体预算提高9倍，也只能解决95%的威胁。这需要企业提高整体安全预算之中只有95%的威胁。在大多数情况下，这样的预算增加对于整个企业来说是得不偿失的。

关于安全措施有一个基本的矛盾：随着安全防护的增加，安全系统的可用性却在下降。也就是说，越安全的系统越没有使用价值。例如，要实现一台移动设备如智能手机的绝对安全。首先需要将设备设置为飞行模式，并将设备锁定在安全模式。绝对安全倒是实现了，可用性也降到了零。所以要保证数据和系统的安全，必须要在有效安全措施和可用性之间进行较量，并达成某种平衡。

实施“深度安全”

因为网络安全的重中之中就是保护好企业的数据，所以好的网络安全措施需要为数据驻留的系统和数据访问通过的网络提供保护。在大多数情况下，企业都应该实行“深度安全”措施。该措施推荐使用多层防护来应对威胁。例如，为了防止网络钓鱼攻击，公司可以对员工进行培训，提醒他们小心打开不明邮件。作为更进一步的安全措施，公司可以将这种培训与杀毒软件结合起来进行培训，如果可能的话，最好是能够检测钓鱼攻击的杀毒软件。

所有敏感的和专有的信息，而不仅仅是这些数据中一部分，都必须要考虑解决和减轻网络安全威胁。保护这些信息资产不仅必须考虑到公司的内部，还要考虑到外部供应商、承包商和其他合作伙伴。由于企业将其数据委托给系统未受充分保护的第三方供应商所导致的安全泄露事件，时常充斥各大新闻网站的头条。

说到安全措施，应该将CIA概念（即前面提到的保密性、完整性和可用性）作为一项基本要求。具体来说，安全控制必须不仅仅是为了解决数据的保密性，还要解决数据的完整性和可用性。要知道，黑客神通广大。如果他们无法获得数据，他们可能会阻止其他人的访问，或者设法破坏数据的完整性。

永远不要低估社会工程攻击和其他类似的“非技术”攻击的有效性。每个公司每天都在经受着网络钓鱼和其他手段的攻击。适当、反复的员工培训是减轻这种实质性威胁的最重要的步骤之一。

可适用的法律和标准要求企业采取合理的措施应对威胁。这意味着要进行适当的能够平衡安全性和可用性的投资。达到适当平衡是设计成功网络安全方法的关键。

（牛安全）

保护银行敏感数据“外发”安全有妙招

目前，各家银行已经建立起越来越多的信息化系统，诸如网上银行系统、财务系统等，但其中的很多研发数据需要外包给第三方合作伙伴，如何保证这些数据的安全已成为金融银行领导亟待解决的问题。

近年来，国内外爆发了多起银行业信息安全事件，从央视315曝光国内某些金融机构客户信息泄密，到韩国农协银行、花旗银行的信息安全事件，给全球银行业数据安全拉响了警钟。与此同时，国资委、公安部、银监会等国家相关部门提出了一系列信息安全相关政策规定，强化银行信息科技风险防范和信息安全保障能力。

银行客户信息一旦泄漏，不仅使企业和个人蒙受损失，也会对社会公众信心造成极大的影响，扰乱整个行业的秩序，甚至有可能影响国家经济的正常运转和社会的稳定。

由此，金融行业面临着各类信息(如用户信息、经营数据、财务数据、人事信息等)防泄漏和研发外包业务系统数据的安全和保密两大难题。

众所周知，银行网络系统的的安全性和保密性要求都比较高，而办公网则较为宽松。

办公网可连接到互联网办公，桌面机普遍存储着需要保护的客户敏感数据和管理报告等电子文件。内部沟通不可避免，信息交差互传频频。随着移动业务的增多，一线人员更多的业务营销活动需要与同业交流，业务数据管理也全面延伸到个人办公终端。

因此，加强办公电子文件安全管理，提升信息安全防护水平已成为银行信息安全管理的核心。数据安全专家敏捷科技分析，银行业面临的主要数据安全风险包括以下几个方面：

1)明文存储存在泄密风险：金融银行(如：研发外包数据、合同、招标文件等)经常已明文方式存储，在传播使用过程中存在泄密风险。

2)明文无法控制使用周期：金融银行的外部交流使用数据通常采用Internet传输，而当对方使用完相关文档后，无法控制电子文档的生命周期，无法判断对方是删除还是外泄导出。

3)外发明文文档易被篡改：金融银行当向外分发大量合同类或研发代码类资料时，存在被人恶意篡改的可能，从而造成银行内部的损失。

4)文件操作无审计无法追溯：银行外发明文数据一旦泄密行为发生后，无法确定泄密源头，无法明确泄密责任。

据了解，敏捷科技文件外发管理系统Agile FD是针对银行企业机密信息或核心资料需要外发给第三方的需求而研发的一款文档外发控制产品。当涉密文档外发给第三方人员时，通过文档外发控制系统生成外发文件发出，通过限定接受者文档使用权限、限定阅读次数和使用时间等方式，来控制外发出去的机密文件，有效避免机密信息的二次泄露以及非法使用潜在风险，解决了企业机密信息被非法扩散的问题。

文件外发管理软件可以解决以下问题：

1.提高管理效率简化解密流程。申请解密表单与需解密文件绑定，通过业务管理人员审批，文档解密动作在外发服务器上完成，大大降低了在客户端解密的风险，同时也避免了手工解密的繁琐过程。

2.防止企业内部合法解密的文件二次泄密。机密文件通过文件外发系统进行“密文解密”后，文件仍然处于加密状态，内部人员获取后，通过任何通讯工具、存储设备带出企业文件仍然是加密状态，文件只对外协单位有效。

3.防止外协单位对机密文件二次泄密。发给外协单位的机密文件都给予了时间、次数等控制，不同的外协单位获取文件后必须通过各自特定的外发浏览插件打开外发文件，而且文件受到严格的权限控制，很好地阻止了文件从外协单位泄密。

（肖波）

智能手机推动中国向4G网络发展

GSMA（GSM协会）旗下的研究机构GSMA移动智库（GSMA Intelligence）7月13日发布了一份新的研究报告，报告指出智能手机在今年年底将占中国移动接入总数的三分之二。这份名为《中国的4G设备如何改变世界最大的移动市场》（How 4G Devices in China Are Transforming the World's Largest Mobile Market）的新研究报告发现，中国的智能手机使用率（占接入数量的百分比）在2015年第一季度末已达到62%，超过了欧洲55%的平均水平。

国际手机品牌（例如苹果的iPhone）和不断增加的国产智能手机的日渐流行促进了中国城镇地区智能手机的快速普及。4G手机现已成为智能手机的销售主力，这加速了中国从3G网络向4G网络的迁移。

GSMA首席战略官Hyunmi Yang表示：“中国几乎近半数的人口为中国贡献了高达13亿的移动连接，其中62%是通过智能手机实现的。我们今天发布的研究报告展现了一个充满活力的中国手机市场，在这个市场中，数以百万计的中国城镇用户将智能手机作为生活的中心和数字平台，同时中国的移动运营商们对4G网络的大规模投资引发了新一轮的增长。”

智能手机正在改变中国的4G市场

GSMA移动智库报告结果显示，2015年第一季度中国的独立移动用户数为6.32亿，占中国人口总数的48%。2015年第一季度，中国市场拥有13亿移动连接，其中智能手机占8.05亿（62%），预计在今年年底将达到9.13亿（68%）。但随着市场的成熟，智能手机连接数的增长在最近几个季度已经放缓，这表明目前智能手机销售的主力来自于换机，而非首次购机需求。

由于手机由3G向4G更替，中国的3G连接已经开始下滑。这份研究报告预测，中国智能手机厂商在2016年之后不会再推出非4G的新手机，而许多厂商现在已经这样做了。据其预测，中国的4G连接将从2014年末的1亿（8%）上升到2020年的10亿，约占三分之二的市场。中国的移动运营商们也在通过其零售渠道向日益广泛的4G设备提供购机补贴，以推动4G发展。

中国智能手机厂商的崛起

根据这份研究，中国的智能手机平均价格为1100元人民币（175美元）。中国国内厂商生产的智能手机的平均价格为935元人民币（150美元），几乎只有国际品牌1765元人民币（285美元）价格的一半。但研究还发现，中国主要的手机厂商，如小米和华为，正在不断地推出面向中高端市场的新机型。

中国厂商生产4G手机的比例也高于国际竞争对手。在2015年第一季度，中国厂商发布的新机型中有70%支持4G网络，而全球平均只有40%。国产4G手机与3G手机之间的平均差价为375元人民币（60美元）。

Hyunmi Yang补充道：“像小米、华为和联想这样的中国智能手机厂商正在从当地丰富的智能手机生产和设计生态系统中受益，让它们能够有效地与苹果和三星等国际品牌竞争。虽然中国持续增加的富裕人群仍然推动着高端智能手机市场的不断发展，但可首次接入移动互联网的低端入门智能手机仍然存在很大的市场。”

（安洁）

大丰收金融联手周六福和太平保险 正式布局O2O线下消费支付板块

7月11日，互联网金融服务平台大丰收金融在深圳宣布与周六福和太平保险合作。大丰收金融将在周六福的全国线下销售网点开设金融理财体验厅，正式布局O2O线下消费支付板块，周六福将为大丰收金融的单个借款项目提供质押物回购保证；太平保险有望为大丰收金融的单个借款项目提供履约保证保险。这两项合作均是互联网金融行业首创，创新了大丰收金融平台P2P安全保障模式。

根据大丰收金融与周六福的战略合作协议，预计未来大丰收金融将在周六福大陆地区的近1500家加盟店及直营店开设金融理财体验厅，将互联网金融融入传统珠宝产业链，有望实现线上线下相融合的O2O循环造血商业闭环，是大丰收金融进军线下消费支付板块的有力举措，深化了大丰收金融“综合金融+线下消费支付平台”模式。

大丰收金融总经理谢海青说，秉承“打造首家极致用户体验的互联网金融平台”为己任，大丰收金融在专注P2P网贷、众筹、供应链金融等综合型互联网金融理财服务的同时，重视用户在生活、购物、娱乐等方面的线下需求，做到线上线下“两手都要抓，两手都要硬”。此次战略合作旨在借由互联网金融平台精准定位、吸纳用户与流量，并连接线下实体产品和服务提供商，构建泛销售圈和泛消费圈，而后基于平台用户大数据基础上，打通消费端、产品端、物流端与资金端的链接，为用户打造集理财、消费于一体的生态社区平台，构建无边界互联网金融生态圈。

严格的风控体系是P2P平台安身立命的看家本领，本次发布会还签署了大丰收金融与中国太平保险的意向合作书。太平保险水贝珠宝支公司副总杨春荣说：“此前P2P平台与专业保险公司的合作模式，仅对平台会员账户资金安全承保，而对P2P平台的单个金融标的实行风险保障，这无论在保险行业还是互联网金融行业来说都是先例。”

据悉，大丰收金融把公信力建设放在运营管理的首位，从平台建立之初就设立了三重风险保障措施：实力雄厚的担保机构进行担保+专业第三方债权收购公司进行债权收购+大丰收金融风险保证金进行代偿，实现100%的投资本息有保障。此次与中国太平保险达成在单个项目上的承包机制意向，将创新业内风控规则，大丰收金融开创的“综合金融+线下消费支付平台”商业模式，也是互联网金融+模式的新探索，未来综合金融板块将不再是大丰收金融平台的唯一收益来源，通过提供其他增值服务而产生的无风险收入将成为大丰收金融的重要盈利点，这种模式颠覆了现有互联网金融的业务模式及盈利模式。

（马爱平）

Dyre已经成为当下金融木马威胁

Dyre金融木马大约在一年前出现，并且目前已成为最有效的金融欺诈工具之一。犯罪分子利用Dyre对全球1000多家银行和其他公司的客户进行欺诈。在英语国家，尤其是美国和英国的客户面临最大的风险，这是因为被锁定为攻击目标的银行大部分位于这些国家。

在Gameover Zeus、Shylock和Ramnit等几个重大金融威胁相继被打击后，由这些组织所造成的威胁已经削弱，但Dyre现在已经取而代之，成为普通客户所面临的主要威胁之一。

赛门铁克公司检测发现，Dyre的文件名为Infostealer.Dyre，以Windows计算机为攻击目标，并且能够通过攻击三款主流Web浏览器（Internet Explorer、Chrome和Firefox）窃取银行凭证和其他凭证。此外，Dyre将构成双重威胁。除窃取凭证外，它还能够向受害者传染其他类型的恶意软件，例如将用户添加至垃圾邮件僵尸网络。

一年内的增长

根据赛门铁克安全响应团队发布的技术白皮书显示，感染Dyre的用户从一年前开始激增。这款恶意软件背后的攻击者不断提高攻击性能，并持续构建支持其发展的基础设施。

由于攻击者的目标不仅仅是为了窃取金融机构的信息，还抱有其他恶意目的，赛门铁克所检测到的活动数量并不能确认为实际的感染数量。赛门铁克发现，一些国家拥有很高的活动数量，但实际受到攻击的银行数量并不高。在过去一年中，赛门铁克检测到中国大约有1236次活动，并未列入前十大受威胁严重的国家，仅有2家银行成为攻击目标。

感染传播途径

Dyre主要通过垃圾邮件传播。在大多数情况下，恶意电子邮件伪装成商务文件、语音邮件或传真消息。当受害者点击电子邮件附件，就会被重新定向到一个恶意网站，该网站将在受害者的电脑上安装Upatre下载器。Upatre是金融欺诈组织最常用的侦测工具之一，此前Gameover Zeus和Cryptolocker组织都曾使用过该工具。它在受害者的计算机中充当桥头堡，收集相关信息以及试图禁用安全软件，最后下载并安装Dyre木马。

凭证窃取

Dyre能够使用几种不同类型的浏览器中间人（MITB）攻击受害者的Web浏览器，从而窃取凭证。其中的一种MITB攻击会将受害者浏览过的每一个网页进行扫描，并对照Dyre预先配置的攻击网站清单进行核查。如果找到匹配结果，该MITB就会将受害者重新定向到与真正网站外观相似的虚假网站。该虚假网站将收集受害者的凭证，然后将其重新定向回原网站。

第二种MITB攻击可以通过添加恶意代码让Dyre篡改合法站点在浏览器窗口中的显示方式，进而窃取受害者的登录凭证。在某些情况下，Dyre还可能会显示一个附加的虚假页面，通知受害者其电脑无法被识别，并需要提供其他凭证来验证用户身份，例如生日、PIN码和信用卡详细信息。

（肖文）