信息安全,与危险同行 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/278/2021_2022__E4_BF_A1_E6_81_AF_E5_AE_89_E5_c101_278274.htm 据社会学家考察，早在远古时代，人类的祖先就已表现出对风险的深深困惑和对其奥秘的孜孜探究，其最发人深思而又最饶有趣味的例子，莫过于“ 轮子 ”和“ 骰子 ”的相伴而行。科技史专家公认，“ 轮子 ”是自“ 钻木取火 ”后人类最伟大的发明，考古发掘已经从墓葬中发现了距今5500年以前的用于运输重物的轮子，以后的纺轮、齿轮、涡轮无不是这一伟大发明的模仿和延伸，可以说人类的早期文明就是借助于火与轮生长起来的。然而，几乎与“ 轮子 ”的发明同步，另一种“ 滚动物 ”“ 骰子 ”也应运而生，而按《大英百科全书》的解释，骰子最初的功能就是占卜，原始人以之预测凶吉，以后才用于赌博。 这是不是可以说明，人类对自己的行为的风险意识是与生俱来的？在人的潜意识里，未知与风险的刺激并不弱于发明和劳作？并且，越是重大的发明，越是有重大价值的行为，也越是风险莫测？ 信息技术的发明和发展，正在以最现代的形态演绎着这一最古老的定则。10月末在常州召开的第17次全国计算机安全学术交流会暨电子政务安全讨论会上，国家计算机网络与信息安全管理中心副主任兼总工程师方滨兴演示的幻灯片让在场的140位与会者心惊肉跳：今年10月上半月，全球仅黑客攻击事件就发生了7228次之多，这还不算肆意泛滥的病毒，莫明其妙的系统崩溃，以及防不胜防的来自地面和空中的窃密者；今年1至3月，观察到的全球病毒扩散次数超过5.8亿次，中国大陆一则发出的扩散次数超过3.13亿次

，全球有33.6万个IP被感染，中国大陆超过8.89万个。而据介绍，国外最新研制出的计算机“ 接收还原设备 ”，可以在数百米、甚至数公里的距离内接收任何一台未采取保护措施的计算机屏幕信息。 信息安全产业的“ 繁荣 ”则提供了另一个佐证。1997年以来，我国GDP的年增长率约为8%，信息产业的增长约为30%，信息安全市场的增长率却超过了50%。其中，1999年安全产品约为9亿元人民币，2000年超过19亿元，2001年超过40亿，今年预计将达到100亿元！另据IDC公司提供的数据，2001年全球信息安全产品市场已高达660亿美元，到2006年，这个数字将增至1550亿美元。该公司对1000名IT经理人进行的调查表明，40%的经理人把IT安全列为最优先考虑的问题，多数人认为“ 安全是IT开支唯一要增加的领域 ”。 难怪信息安全企业近年来如雨后春笋（国内信息安全企业已由2000年的300家增长到现在的1300余家），也难怪信息安全市场会成为包括联想、瑞星、紫光、金山、东大阿尔派等在内的厂商们“ 鏖战 ”的新热土。 易思克网络安全技术公司总工程师邵通接受笔者采访时甚至断言：“ 下一轮计算机的换代将不是因为速度，而是因为安全！ ”正视“ 不安全文化 ”然而，当人们静下心来思考信息安全的对策时可能会沮丧地发现，自己首先需要解决的问题似乎不是如何根除危险，而是如何“ 端正思想 ”，即如何“ 容忍 ”危险，学会“ 与危险共存 ”。因为从根上说，危险是不可能一劳永逸地解除的。 科学家早已告诫，人类智力的进步并不意味着风险的化解，因为这种进步会鼓励人们不断把触角伸向新的、风险莫测的领域。人们甚至发现，如果把已知的事物看作一个圆，圆周之外为未知之物的话，则“ 所知越多，圆周越长，与未

知之物的接触面也就越大，从而遇到的风险也越多越频繁 ”。 在这个意义上，今人面临的风险并不弱于古人。古人固然享受不到计算机网络等新技术带来的方便、效率和财富，可也绝对不会遭遇核武器、生化武器、克隆人、网络战等可能带来的灾难和荒恐，更不会想到，“ 9.11 ”后“ 打开一封信都可能是一种致命的危险 ”。 于是人们便不无兴趣但又并不轻松地看到，当网络专家们兴奋地论证着“ 网络效应与结点的增多成正比 ”时，站在一旁的安全专家却忙不迭地告诫“ 网络结点越多网络越脆弱 ”多一个链接就多一分被黑客和病毒攻击的危险。 信息安全的话题在这儿似乎成了一个无解的悖论。一方面是人们忙忙碌碌地寻找着各种各样的网络解决方案，另一方面却是“ 连网本身就是最大的不安全 ”。 有位反病毒专家在一个研讨会上发问“ 谁的电脑没有感染过病毒 ”？台下一百多号听众中竟没有举起一只手来。由此得出的结论只能有两个：其一，信息技术的发展与危险的发展如影随形，此长彼亦长；其二，如果有谁想追求“ 百分之百的安全 ”，办法只有一个，就是把自己关进信息孤岛。这显然是人们不愿意的。 信息安全专家、中国现代国际关系研究所信息与社会发展研究室主任俞晓秋曾忧心仲仲地谈到信息革命给现代社会带来的“ 脆弱性 ”问题。的确，当一个社会从经济到文化，从工作到生活，从军事到政务都已离不开信息技术，而信息技术又隐藏着巨大且不可能根除的风险时，这个社会的“ 脆弱性 ”也就无可怀疑了。现在面临的问题已不在于这种脆弱性的有无，而在于如何控制这种脆弱性，减少风险“ 发作 ”的次数和强度，把对信息安全的威胁降到社会可以接受的限度以内。而信息系统的脆弱性涉及技术、应用、管

理等多种因素，包括让你防不胜防的天灾人祸。即使你采用了世界上最好的安全产品，内部管理慎之又慎，也难保万一。遭遇“ 9.11 ”的一家美国公司为保证信息安全而斥巨资建立了数据备份中心，却毁于百密一疏之中它把备份系统放到了世贸中心另一栋大楼里，想不到两栋大楼都在恐怖袭击中化为灰烬。 我们还知道，保障信息安全是以牺牲方便性、灵活性为代价的。如同你给家里装了一把很复杂的门锁，小偷是撬不开了，但你自己进门也麻烦了许多，忘记了密码还会把自己锁在门外。为信息安全的层层加密不仅会抬高成本，还会影响系统运行速度。通常情况下人在电脑屏幕前等待的耐心只有7秒钟，如果因为安全而降低了工作效率，不少人宁可放弃安全。著名社会学家、慕尼黑大学教授乌尔里希贝克就曾批评布什政府所主张的对恐怖分子的全面控制方针“ 显然是不可能的，而且最终可能导致失望，产生相反的结果 ”。在这里，“ 不安全文化 ”成了解决信息安全首先需要正视的事实。乌尔里希贝克据此提出，当今社会应当“ 发展一种不安全文化 ”，在他看来，零风险如同零失业率一样，充其量不过是一种“ 集体的谎言 ”。如果承认此话有些道理，那么我们的信息安全策略就须把“ 不安全文化 ”纳入其中，作为思考和应对信息安全问题的重要参考系。这其实也就是管理学所说的风险管理的思路。安全厂商常常会信誓旦旦地给用户作出“ 全面控制 ”、“ 万无一失 ”的保证。但这是不可能的，你也千万别信。再深一步看，“ 不安全文化 ”还涉及人们承担风险的意识，而这也是发展和应用信息技术所必不可少的。期望一切都在理性的控制之内，期望绝对安全了再去投资或应用，所付出的代价会更大。著名经济学家凯恩思就

曾说过，假如一个人生性不喜欢碰运气，而仅靠冷静盘算，恐怕不会有所作为。美国学者乔治吉尔德甚至认为，一个社会获得成功的主要秘密，也许在于它把追求安全转变为愿意冒险的能力。在这里，对危险的承认和控制，而不是对危险的一劳永逸地根除的意愿，构成了“ 不安全文化 ”的基础性内容。 信息安全的两个视角 由操作层面看，既然“ 不安全文化 ”视不安全为一种常态，对信息风险的防范理所当然地就应当纳入企业和社会日常管理的轨道。在第17次全国计算机安全学术交流会暨电子政务安全讨论会上，来自公安部、总参谋部、信息产业部、中科院等数十家单位的140多位专家、企业家和政府官员，就信息风险的防范深入交换了意见，归纳起来有两个大的视角：战略视角、经济视角。 在战略视角方面，中科院院士沈昌祥强调信息安全是一项包括技术层面、管理层面、法律层面的社会系统工程，延伸开来还应包括观念和文化层面，例如从文化意义上构建信息技术的行为准则，培育网络空间的道德规范。我国已经颁布了一系列有关信息安全的管理条例，但还缺少国家级的统领全局的信息安全框架，这不能不说是一个巨大的缺憾。他介绍，“ 911 ”后美国信息基础设施保护委员会（PCIPB）列出了53个信息安全重点问题，把信息安全列入国家战略。在这个战略中，信息安全保护被分成5个等级：第一级是家庭用户与小型商业机构，第二级是大型企业，第三级是高等教育、联邦政府、州与地方政府等关键部门，第四级是国家优先任务，第五级是全球性合作网络。五个等级五种保护模式，如第一级保护只要求采用密码、过滤、防病毒软件等技术，使用高速连接设备的还应考虑防火墙；第五级保护则包括建立广泛的“ 安全文

化”，推动国际化合作网络的发展，在安全事件初露端倪时便能通过该网络进行确认并提供防护。