面临当前日益复杂的网络安全现状挑战，所有组织都有必要增强日常的网络防范意识。**“被黑客成功攻击，并不一定意味着对方的技术有多高明；而很可能是因为我们本可以采取的预防措施没有做到位。”**

部门规章、地方立法以及行业标准等。

“个人用户在网络安全上对企业的不信任归根结底是由于保障制度的不明确。上述法律法规等规范性文件的落地过程中，对大众进行法律的普及和解释的工作，任重道远。”惠志斌表示。

他提出：在法律体系之下，其实在用户个人的数据安全管理方面，人们对拥有庞大的用户信息资源的互联网大企业是不用过于担心的，因为他们需要确保“数据合规”来建设自己的核心竞争力。也就是说，法律法规相当于明确了红线，使得企业与个人之间的数据活动有了可遵循的章法，这对于规范整个行业的安全、保护用户个人信息来说是显著利好的。

来自政府层面的监管对于个人和企业而言当然是必须的，但并非“一管就灵”的妙药。因为在数据爆炸的当下，不可能把所有监管都交给政府来做，那样必然让政府不堪重负；互联网平台也要承担部分类似政府的监管责任。例如，《个人信息保护法》草案二次审议稿就提出：互联网平台对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务。这一规定，与《电子商务法》中规定的平台经营者对平台内电子商务经营者相关产品质量、知识产权、消费者保护的监督责任类似。

将来，网络数据安全将在用户、企业平台和政府三者的互动中取得动态平衡，逐渐取得最优解。

## 网络安全人才的培养

在“数字主权”意识兴起、“数据安全”成为热点话题之外，攻防对抗依然是网络安全中非常关键的一部分。公安部第三研究所主要从事网络安全与智慧警务科研创新与技术支撑，专攻网络攻防、网络侦查、技术侦查、国产密码、电子取证、等级保护、大数据分析等领域。该研究所下属的公安部国家级专业技术人员继续教育基地（简称“教育基地”）副主任黄镇告诉《新民周刊》记者：当前全球范围内网络安全的攻防对抗仍然十分激烈。

他表示：趋利性增强是近年来网络攻击的一大特点。“以前我们遇到的‘黑客’发动网络攻击有不少是为了证明自己的技术水平，是一种‘炫技’；或者是为了发泄某种情绪而有所行动，并不涉及经济利益的诉求。但是，当前为了经济利益而发动的网络攻击越来越多，而且攻击者背后存在团伙体系，形成了网络攻击的利益链。”

勒索病毒就是这种网络攻击的代表。感染该病毒的电脑会连接至黑客的服务器，上传本机信息并下载加密所用的密钥，之后将本机所有关键的数据文件加密，让用户无法打开。勒索病毒还会在桌面壁纸、弹窗等位置生成提示，要求用户交纳高额赎金，才可恢复文件。黑客选择了比特币等虚拟货币收款方式，使得其账户无法被追踪。实际上，交纳赎金也并不能保证数据文件得到恢复。

2017 年 5 月 12 日，一种名为“想哭”的勒索病毒袭击全球 150 多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。这是近年来勒索病毒流行的开端。之后的几年里，各种不同的勒索病毒在全球范围内不时出现。

不幸感染勒索病毒也并不意味着只能向黑客屈服，但此时再寻求破解黑客的加密手段，难度确实比较大。黄镇打了一个比方：防勒索病毒就像防止坏人对仓库大门的控制。我们在平时就要把门锁加固、在门口安装监控和警报等装置、多加巡视检查，并且主动了解坏人最新的攻击方式。如果这些工作在之前没有做好，就容易让坏人把我们的门加上他的锁。此时，我们又想进仓库拿货物，又不想把大门以及与大门紧连的货物破坏，就很难了。当然，如果我们之前把同样的货物备在别的仓库里了，此时就可以应急。

实际上，不仅是应对勒索病毒，面临当前日益复杂的网络