网络安全

我国网络安全现状

企业面临的网络风险或者网络威胁主要有以下几种形式：

- 网站入侵、网页内容篡改

表现形式：黑客利用网站漏洞侵入网站，篡改网页内容，甚至贴上反动标语。

后果：造成严重的政治影响，对企业公关形象产生负面影响，被监管部门处罚，影响正常业务开展。

- 数据泄露

表现形式：生产运营中积累大量客户数据的企业遭受黑客攻击，数据被窃取并用于非法用途。

后果：面临监管处罚。此外，还可能面临第三方的索赔。

- 网络勒索

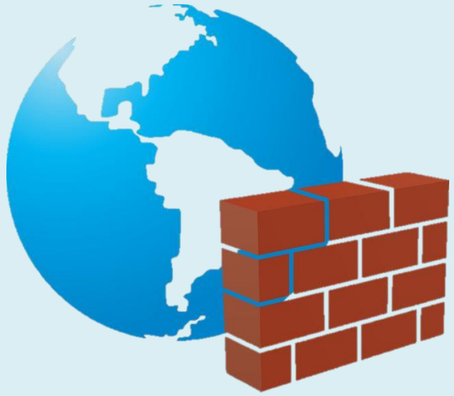
表现形式：遭受网络勒索软件攻击，需向对方支付勒索金后方可解锁相关软件或数据。

后果：支付勒索款项造成经济损失；或者生产经营中断造成营业中断损失，营业中断损失是目前大家公认的网络安全风险中最大的风险。

- 分布式拒绝服务攻击

表现形式：网站受到来自多个站点的同时攻击，使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的网络服务。

后果：网站无法提供正常服务，通过网站接受订单服务被中止，同样造成营业中断的后果。



国际网络安全现状

全球网络攻击事件更加频发

1. 一是软硬件设备安全漏洞频出给生产生活带来严重威胁。1 月，英特尔公司爆出“幽灵”“熔断”两个处理器漏洞，导致恶意程序可获取敏感信息。英国皇家战略研究所公布报告，指出当前核武器系统存在大量明显安全漏洞，网络攻击破坏核武器控制装置的风险极大。
2. 二是多行业关键信息基础设施遭受攻击。1 月，荷兰三大银行网络系统在一周内不断遭受分布式拒绝服务攻击。6 月，美国赛门铁克公司发现黑客组织针对美国和东南亚国家卫星通讯、电信、地理太空拍摄成像服务和军事系统进行网络攻击
3. 三是个人信息与商业数据遭遇大规模泄露与违规利用。4 月，美媒报道特朗普大选期间聘用的“剑桥分析”从 2014 年起违法收集脸谱网上 5000 多万名美国用户的数据，用于预测和影响选民的大选投票取向。

我国网络安全目前存在的问题

我国网络威胁监测技术仍待加强

一是信息技术安全监测能力不强。我国对进口网络信息技术和产品的监测分析以合规性评测为主，很少涉及软件核心技术，规模化、协同化漏洞分析评估能力较低，难以发现产品的安全漏洞“后门”，同时在大数据分析、可信云计算、安全智能联动等重要方面的技术实力不足，难以应对新兴信息技术产品的安全监测工作。

二是网络攻击追溯能力不足。目前，我国对于海量网络数据缺乏有效的分析方法，对 APT 等新型安全威胁的监测技术不成熟，即便监测到这种威胁，由于缺少回溯手段，也难以找出攻击源头。

如何防范网络安全

（1） 禁用不必要的端口和协议，端口是与外部网络相连接的，它的正确配置与否直接影响到 计算机的安全。

(2)不需要文件和打印机共享的电脑，可以取消共享功能。

(3)数据加密技术，数据加密是将一个信息(明文)经过加密及加密函数转换，转换为没有意义的另一个信息(密文)。

(4)防火墙技术，防火墙的含义是一个或一组系统，用于加强两个不同之间网络的访问控制，是两个不同网络之间的网关。

(5)身份认证技术，一般包括身份认证和身份识别两方面，它是确认通信双方身份真实性的 重要步骤。