安永发布《2021 安永全球信息安全调查报告》

（来源：安永微信公众号）

安永今日发布《2021 安永全球信息安全调查报告（GISS)》(以下简称《报告》)，揭示了企业在全球疫情背景下的信息安全面临着诸多威胁与挑战，并针对性地提出化危为机的解决方案。该报告是安永持续第 23 年发布的全球信息安全调查报告，旨在探索当今企业所面对的最重要网络安全议题。报告显示，新冠疫情催化了云计算等技术的应用以及办公场景的变革，企业因此需要应对更加复杂多样的网络安全风险，然而超过四分之三的中国受访企业（75%）不确定其网络安全防御体系是否足以应对黑客的攻击。

安永调查表明，网络安全职能部门在力争成为业务发展推动力和业务战略合作伙伴的道路上，疫情危机使其遭受了极具破坏性的巨大挑战。在全球疫情好转之前，局势仍可能会进一步恶化。企业需要在后疫情时代加大技术和创新层面的投资，确保具有足够的韧性面对下一次大规模网络破坏。

安永[1]大中华区咨询服务主管合伙人王海瑛表示:“新冠肺炎疫情给企业的信息安全团队敲响了警钟，在信息安全问题愈加严峻之际，信息安全职能比以往任何时候都受到重视，信息安全团队将借此机会更好地表明其角色的战略重要性，提升在企业中的形象。”

本次调查对全球逾千位首席信息安全官和其他高管进行了调研访谈。基于《报告》结果，企业首席信息安全官正面临着诸如缺乏高层重视、预算不足、多头监管、跨团队沟通待增强等方面的问题。自 2020 年发布上一期调查报告以来，高破坏性且高复杂度的网络攻击

数量开始大幅增长，首席信息安全官肩负着更大的压力，企业也面临着更大的网络风险。除此之外，预算限制意味着首席信息安全官需要努力缩小需求和资金之间的缺口。

全球合规环境正变得越来越复杂，某些行业（尤其是金融服务业）的企业还必须应对特定行业的监管。**安永中国金融服务科技咨询服务主管合伙人阮祺康**表示：“对于国际组织而言，应对这些互为重合又时有冲突的监管规定将会变得极具挑战性，尤其在数据变得无所不在并且全球流动的情况下。”

面对这一系列问题，**安永大中华区网络安全与隐私保护咨询服务主管合伙人高轶峰**表示：“企业的信息安全部门应发挥更加积极的作用，在企业投资决策的最初阶段提供咨询建议，以更好地满足后疫情时代不断变化的业务需求。同时，企业应当意识到这不仅仅是 IT 部门或安全部门的工作，只有企业中各方利益相关者相互配合、各司其职，才能快速、有效、从容地应对监管合规带来的压力和挑战。”

网络安全投资与需求不同步

当前，网络攻击威胁日益严峻，网络安全风险已达到峰值。攻击者的目标越来越多，采用的攻击方式也愈加难以预测。尽管如此，相对于整体信息技术支出，多数企业的网络安全预算仍与需求存在较大差距。

调查数据显示，虽然约三分之二（67%）的中国公司表示诸如勒索软件等破坏性网络攻击的数量在过去 12 个月中有所增加，但应对网络安全风险的预算仍然很少。近一半的受访者（45%）比以往任何时候都更担心公司是否能够应对网络威胁，这一数据与全球平均数值（43%）相近。此外，约五分之二（40%）的中国企业预计将遭受重大

网络安全事件。因此，对中国公司而言，更应积极主动地在网络安全防御方面适当投资，以避免企业遭受到重大网络安全破坏。

安永大中华区网络安全与隐私保护咨询服务合伙人兰瑜表示：“为了在后疫情时代寻求业务转型和创新发展，许多企业正在计划新一轮科技投资。如果网络安全被排除在投资讨论之外，那么未来几年网络威胁将持续增长。企业应考虑将网络安全成本分摊至整个企业，使网络安全成为一种推动力量，为企业的转型升级保驾护航。”

“多头监管”为信息安全团队带来更加严峻的合规挑战

安永大中华区网络安全与隐私保护咨询服务合伙人施建俊表示：“全球合规环境的愈加复杂及监管力度的加强是目前不可避免的趋势。“多头监管”可能在较长一段时间内都会是企业要面对的问题，特别是对于跨国企业而言，了解复杂的、动态发展的、相互影响的国际监管格局更是一项严峻的挑战。”

中国54%的受访者认为确保合规是工作中压力最大的部分。同时，中国67%的受访者预计，监管在未来几年将变得更加多样化，对于符合监管所做的工作将花费更多的时间，该比例明显高于亚太水平（54%）及全球水平（57%）。特别是近期《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》的相继出台与生效，更是给在华企业带来了合规的挑战。

危机应对：赢得高层重视并与业务团队建立更紧密联系

此次调查显示，信息安全部门与企业其他职能部门之间的本质关系缺乏能动性和稳固支撑。

中国近77%的受访者表示，在项目规划阶段结束之前，企业往往不会及时咨询信息安全团队或向其汇报情况，这一比例与全球平均水

平（76%）基本持平。

在中国，仅有16%的企业将网络安全纳入所有数字转型计划的规划阶段。受访者认为，虽然各业务线认识到了网络安全的传统优势（如控制风险），但仍未能将网络安全职能部门视为持续长期的战略合作伙伴。

总结

企业应当根据其核心目标和潜在风险来制定业务规划，以确保信息安全团队、首席执行官和最高管理层及其他成员之间保持一致并维持稳固的战略关系。同时，在中国的愈加严厉的监管环境下，企业要建立符合《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》这三大法案的治理体系，自上而下地从战略、高级管理层责任制进行配套设计，并从人员、组织、技术和流程方面进行落地实施。

[1]安永（中国）企业咨询有限公司