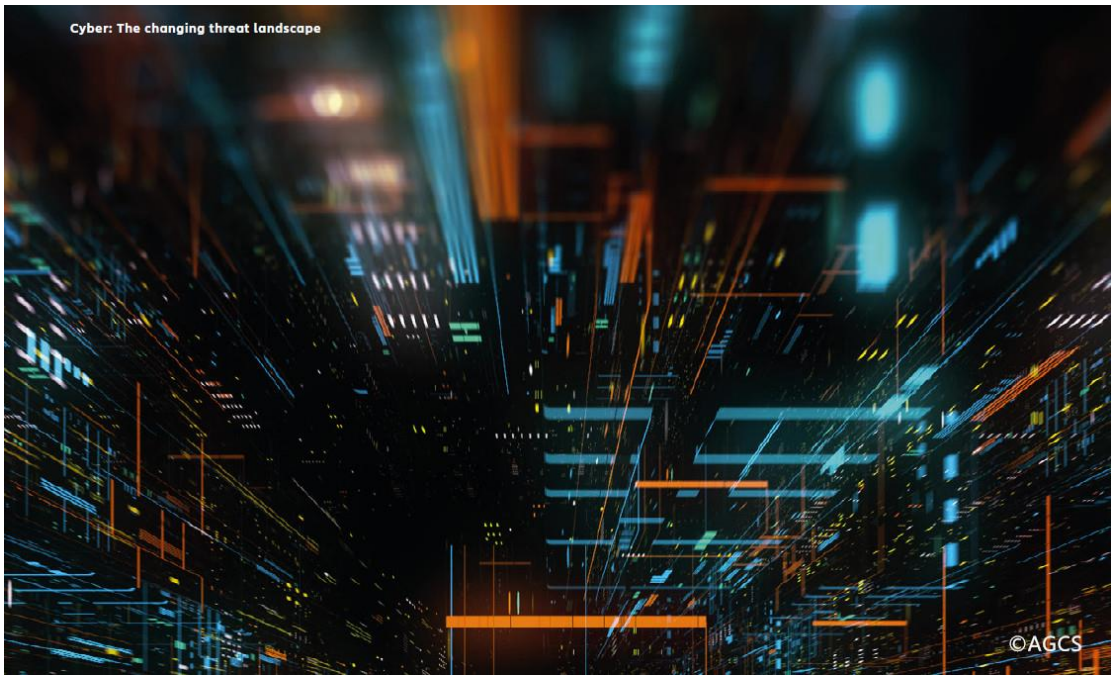
# 【风险提示】安联数据揭示网络犯罪的严重性

作者：王勇




**摘要：**

安联（AGCS）2022 年度调查报告显示，网络风险俨然成为全球最大的商业风险。在过去五年里，安联一直在全球各地参与保险业的相关索赔。从商业承保、理赔和风险咨询三方面进行分析发现，勒索软件攻击成本不断上升，针对中小公司的黑客攻击频发，深度伪造的商业电子邮件欺诈行为频发，以及更广泛的地缘局势影响正成为网络风险的主要发展趋势。这份报告也给集金融贸易和物流运输于一体的航运企业和会员公司敲响了警钟。在互联网通讯、数字化办公为主流手段的管理运营中，不得不加强对网络犯罪事故的及早防范。

## 一、威胁


■ 安联全球网络索赔主管强调，数字化正在深入企业和供应链，IT 外包和云技术的广泛使用，虽然提高了工作效率，但也在增加网络环境的威胁，造成漏洞以及增加互连性和风险的集合。

■ SonicWall’s 网络威胁报告统计，尽管有执法部门的努力干涉，但勒索软件攻击始终是魔高一丈。安联网络风险专家强调，以目前公司的防御技术，不可能阻止每一次的网络攻击，从潜在客户提交的公司防御能力报告来看，有超过一半的客户无法满足安联的网络防御要求。

■ 由于团伙使用越来越复杂的攻击工具和勒索技术，他们将目标锁定在大型公司、关键基础设施和供应链上，使得勒索软件索赔的严重程度逐年上升。在传统的勒索软件攻击中，犯罪分子渗透网络并使用恶意软件对文件进行加密，要求赎金以换取文件的恢复。然而，双重敲诈勒索攻击还包括窃取敏感数据，然后将其用作敲诈勒诈的杠杆。而三重敲诈勒索则更进一步，犯罪分子向商业伙伴、客户或供应商提出敲诈要求，这些可能会受到最初攻击中被盗数据的影响。现在，双倍或三倍勒索已经成为常态，这可能会大幅增加袭击成本。

■ 所有行业中的所有公司都将面临勒索软件的攻击，随着大公司对网络安全的加强，中小企业和公司往往缺乏对网络安全和风险管理的资源投资，从而使得中小型企业和公司成为网络犯罪分子更具吸引力的目标。

■ 在各个行业，继续发生着针对基础设施薄弱或暴露的组织的高调网络攻击，而如今被人们习以为常的远程办公、在线会议和公司对第三方供应商的依赖更加剧了网络攻击的情况。

■ 针对商业电子邮件的攻击变得更加复杂和有针对性并呈现上升趋势，这种攻击将导致财务损失或更具破坏性的网络攻击。

■ 网络战争或冲突更难定义难以归因，尤其是在国家之间发生的网络战争或冲突可能对数以千计的公司造成难以想象的破坏，甚至是破坏关键人群基础设施，如公用事业、通信或支付系统。

■ 另一个令人担忧的趋势是黑客瞄准了脆弱的供应链，此类攻击更应是保险市场特别关注的问题，因为一次网络攻击可能会导致全球数千家公司遭受连锁损失。

■ 网络安全专业人员的短缺同时阻碍了网络安全环境的改善。

## 二、数据


■ 根据 McAfee & CSIS 最新报告，网络犯罪事件现在估计使全世界每年付出超过 1 万亿美元的经济代价，约占全球 GDP 的 1%。

■ SonicWall’s 网络威胁报告统计，在 2021 年，勒索软件攻击次数达到创纪录的 6.23 亿次，预计到 2023 年，勒索软件将给全球组织造成 300 亿美元的损失。

■ 数据表明，网络罪犯在 2021 年勒索的金额平均高达百万美元，而勒索软件服务工具仅需每月花费 40 美元，这使得犯罪成本极低，使用勒索软件犯罪也不需要太高的技术水平，犯罪分子们往往获利匪浅。

■ 根据 Paloalto 勒索软件威胁报告，2021 勒索金额增加了 144%，平均付款增加了 78%。Sophos 的数据显示，约有 46%的公司为了恢复数据而支付了赎金。制造业和公用事业尤其容易受到勒索，面临的赎金最高，平均为 200 万美元。

■ 根据 CipherTrace 的研究，2021 年双重勒索软件攻击增加了近 500%，而支付给勒索软件团伙的款项在前六个月增加了 42%，达到 5.9 亿美元。

■ 2022 年上半年，中小企业的网络索赔平均成本上升了 50%以上。一家非营利性网络研究机构在对 1400 家中小企业的调查中发现，全球 55%的企业尚未建立多元化验证保护机制，这就是目前的网络生态现象。相反，他们只依靠用户名和密码来保护自己的系统，使其非常容易受到网络攻击。

■ 根据 FBI 的数据，2016 年 6 月至 2021 年 12 月，全球针对商业电子邮件诈骗总额为 430 亿美元。

■ 2022 年，Thales 云安全报告显示，约三分之二的组织将其 21%-60%的敏感数据存储在云中，其中约 45%的组织表示他们曾经历过一次数据外泄或未通过数据和云应用的审核。

■ 根据 Cybersecurity Ventures 统计，2013 年至 2021 年间，全球网络安全工作岗位需求增长了 350%，空缺数量达到 350 万个。

## 三、赎金

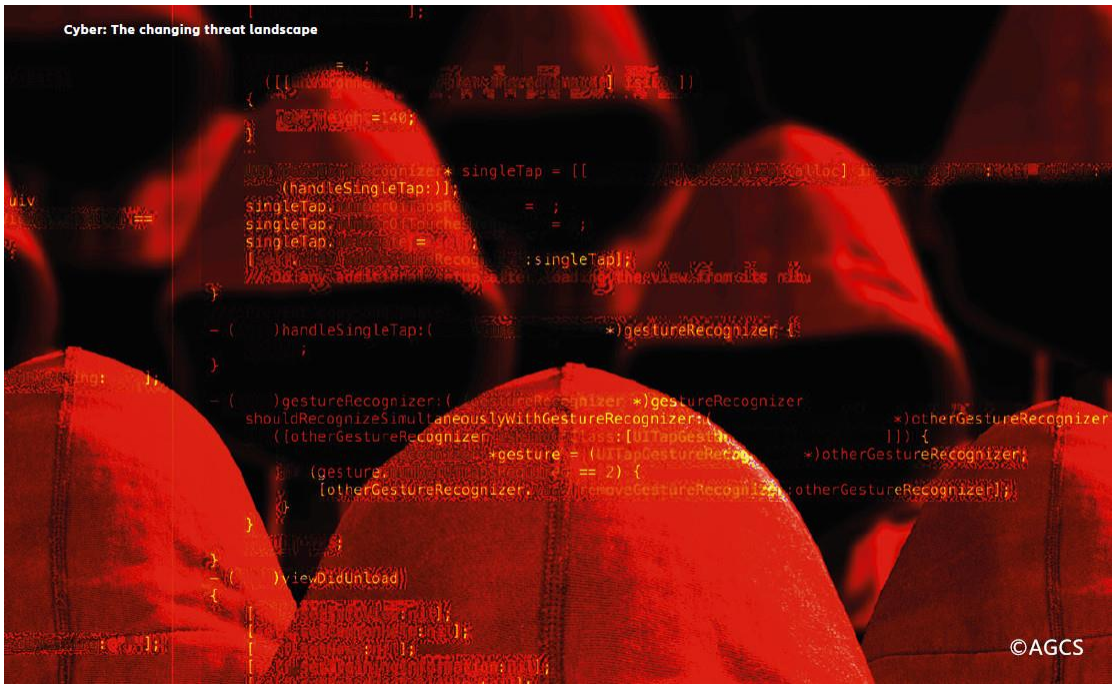
■ 备受瞩目的破坏性网络攻击，已将勒索软件提上政治议程，引发了执法的加倍努力。人们的注意力也转向了支付赎金的要求，新的规则和潜在的禁令即将出台。美国财政部在 2020 年表示，向受制裁的黑客支付勒索软件可能是非法的，并在 2021 年警告各组织在支付赎金时不要违反制裁规则。欧盟成员国可以根据《网络和信息系统安全指令》（NIS 指令）对支付勒索的行为处以罚款。Gartner 预测，到 2025 年，30%的国家将通过监管勒索软件支付、罚款和谈判的立法。

■ 支付赎金是一个有争议的话题，关键服务提供商，如医院或电力公司，除了支付赎金以避免造成严重破坏之外，可能别无选择。另一方面，支付勒索赎金可能会鼓励进一步的勒索软件攻击。制裁规则和恐怖主义条例也可能禁止向某些国家、团体或个人（包括网络团体）支付赎金。

■ 安联风险咨询全球网络专家负责人表示，围绕赎金支付的潜在法律变化不太可能完全解决勒索软件的问题，但可能有助于提高公司应对网络勒索的成熟度，对赎金支付的更严格监管可能会导致网络犯罪分子将注意力转移到其他形式的攻击上，如数据盗窃或供应链攻击，以及更有针对性的攻击。

■ 任何受到勒索赎金影响的公司应始终通知警方或国家调查机构并与之合。

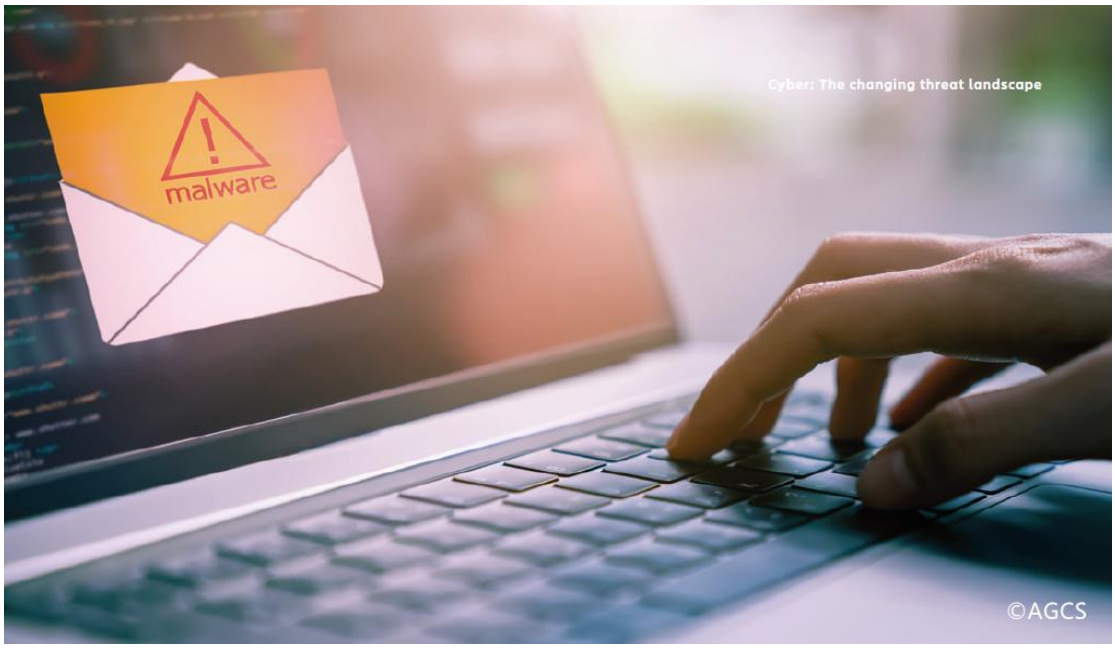
## 四、防御



安联也提出一些对勒索软件的防护措施，一个公司良好的 IT 安全环境应该具备：

- 对勒索软件进行及时有效地识别。
- 对勒索软件事件的响应流程完善且执行到位。
- 对反钓鱼软件的演练和用户安全意识培训。
- 对系统加密和定期备份以及关键系统的频繁备份。
- 对所有移动设备和终端系统的端点保护、端点检测与响应。
- 对电子邮件、web 和办公文档的安全管理。
- 对网络包括云内的物理和逻辑隔离。
- 对监控修补和漏洞管理策略的落实。
- 对新整合的实体进行尽职调查和风险管理评估。。

**五、结语**




长期以来，网络安全一直被视为一个 IT 问题，但如今蓬勃发展的数字经济意味着问题并不止如此。无论是居家办公的兴起、数字化的加速、还是地缘政治等事件的深远影响，网络安全暴露出的潜在和存在的漏洞都变得非常明显，这也将其上升为一个环境安全、社会影响和综合治理的问题。包括公司管理层、投资决策在内的利益相关者应积极重视网络安全，在加强网络防护的同时，也可以考虑网络风险转移等替代解决方案，以提高网络安全成熟度。

以上仅供会员参考，如需了解详情，请参安联报告原文 Cyber: The changing threat landscape。