开展网络安全反击战

文 / 安 · 布莱迪 By Ann Brady

网络攻击给企业、政府和社会带来损失、破坏以及日益严重的威胁。幸运的是，我们可以拿起标准这一武器打赢这场战争。

网络犯罪率不断攀升。在我们大踏步迈进数字时代，即第四次工业革命时代的同时，网络犯罪变得更加复杂、恶劣，后果十分严重。由于网络不法分子越来越狡猾，网络犯罪也在以各种方式渗透进所有人的生活。

网络攻击涉及的范围很广，包括入侵系统和社交媒体、钓鱼式攻击以及恶意软件，如：勒索软件、身份信息盗用、社会工程攻击和拒绝服务攻击等。网络攻击会让个人和经济遭受打击，造成难以估量的损害和破坏，使社会和民众岌岌可危。计算机安全软件公司 McAfee 的调查显示，网络攻击造成的损失越来越大，仅在 2020 年就高达约一万亿美元。

日益严重的全球风险

新冠肺炎疫情让我们愈加依赖数字系统，因此《2022 年全球风险报告》再次将网络安全威胁列为全世界面临的日益严重的风险之一，这也在意料之中。该报告认为，网络安全防御失效的情况愈演愈烈，威胁到长期的繁荣稳定。

但我们如何赢得这场战争呢？建立良好的网络防御系统和预测风险都是打击网络犯罪的重要方法，但如果没有先进、可信的网络风险管理计划，网络安全的治理和韧性就无从谈起。“网络犯罪在国家和国际层面蔓延速度极快，会影响到企业、政府甚至整个社会。由于网络罪犯使用技术基础设施实施跨国犯罪，这种犯罪活动范围广、情况错综复杂，其影响深远，后果严重。”网络安全专家爱德华·汉弗莱斯博士（Dr Edward Humphreys）说。

> **网络安全防御失效的情况愈演愈烈。**

因此，国际协作非常重要，国际标准对全球网络防护而言必不可少，他补充道。这是汉弗莱斯博士基于多年从业经验得出的结论。他身为网络风险、网络安全、网络心理研究以及信息安全管理体系创新研究领域的高级研究员，也是

ISO/IEC 信息安全管理体系工作组的召集人。该工作组负责制定、管理和维护 ISO/IEC 27000 信息安全管理体系系列标准。

解决方案和控制手段

汉弗莱斯博士认为，国际标准提供了解决方案，使组织机构可以建立用于评估、管理的框架和体系，以此保护信息，确保应用、服务以及国家基础设施安全。

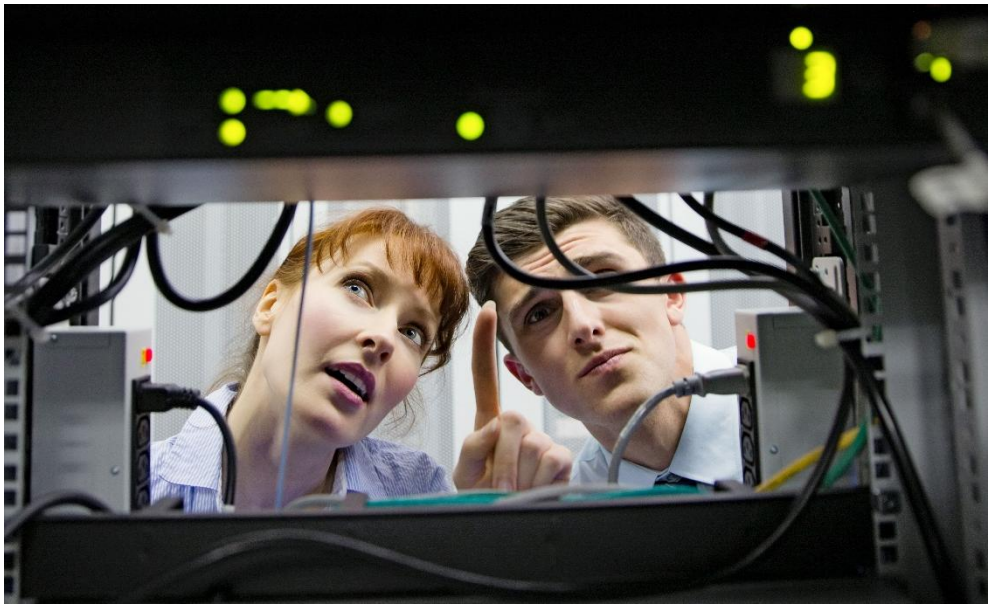
打击网络犯罪的第一步是了解风险，然后决定采取哪些控制手段来减轻风险。汉弗莱斯指出，对于寻求健全的解决方案来打击网络犯罪的组织机构来说，ISO 与国际电工技术委员会（IEC）共同制定的 ISO/IEC 27000 等标准是绝佳选择。该系列标准详细规定了一套管理体系，该体系可以融入评估风险和确定风险控制手段的风险管理流程。

“ISO/IEC 27001 有一系列的配套标准，例如 ISO/IEC 27005 信息安全风险管理标准和 ISO/IEC 27003 实施指南标准。”他说，“此外，还有很多其他标准能为 ISO/IEC 27001 提供技术支撑，如：保障联网安全，将安全功能嵌入技术、服务和应用程序之中。”

时刻做好准备

汉弗莱斯博士再次强调，企业要做好应对攻击的准备。他说：“网络攻击随时随地都可能发生，我们可以肯定的是攻击一定会发生，但无法确定具体的时间或地点。做足准备、未雨绸缪才是企业的生存之道。这要求企业建立一套流程，能预测、识别、发现和报告攻击事件，对其进行分析以制定应对策略。”响应要快速、及时，以减少攻击事件带来的影响。

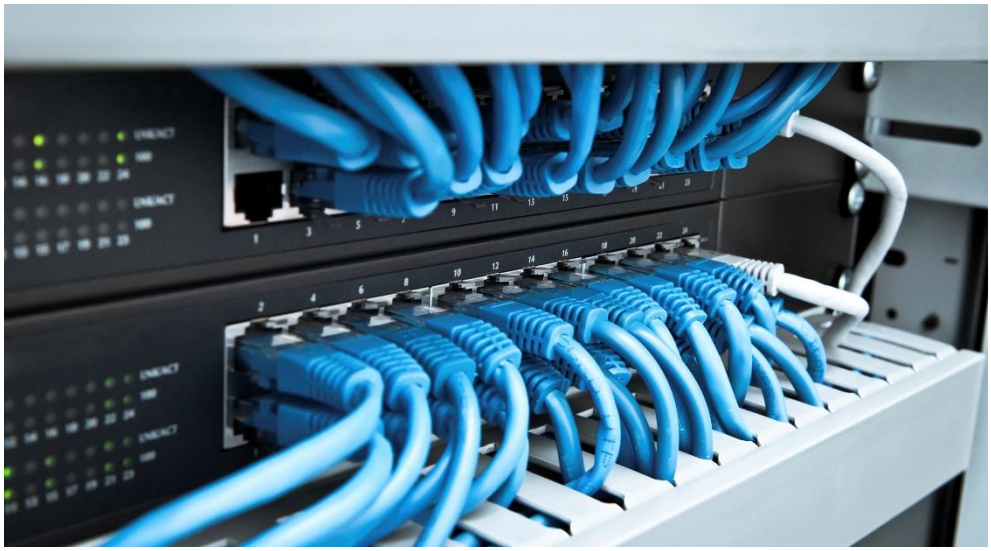
那么，如何更好地防患于未然呢？一旦发现恶意代码攻击或拒绝服务攻击，企业采取适当安全措施的响应速度越快，遏制攻击扩散、减少影响和破坏的可能性就越大。汉弗莱斯博士认为，标准能帮助企业做好准备，更好地应对，这些标准包括 ISO/IEC 27035 信息安全事件管理标准、ISO 22301 业务连续性管理标准和 ISO/IEC 27031 信息和通信技术业务连续性准则标准。



一起行动

在这个充满不确定性的世界，网络犯罪会在经济上对企业经营和国家基础设施造成极大破坏，还会影响到社会和公民。例如：对供应链某一环节的攻击可能会蔓延开来，给其他环节也造成影响和破坏。为了建立更安全、更具韧性的网络安全系统，汉弗莱斯博士认为，供应链所有环节都应采取行动以确保安全。因此，供应链管理是齐心合力一起行动的例证。

“当然，标准也能保障供应链安全，例如：ISO 28000 和 ISO/IEC 27036。”他说道，“在与其他组织机构建立各种业务关系和沟通时，也需要采取共同行动。很多管理标准能帮助企业增加韧性来应对业务中断，并确保企业保持生命力和治理体系稳固。此类标准包含 ISO 22301 业务连续性管理体系标准、ISO/IEC 27001 信息安全管理体系标准和 ISO/IEC 27014 信息安全治理标准。”



随着企业越发依赖互联性，提供支撑的基础设施、互联网和移动设备也逐渐增加，这对系统安全和韧性提出了更高的要求。汉弗莱斯博士坦言，标准也需要不断更新，才能赶上技术飞速发展的步伐。“举个例子，第三版 ISO/IEC 27002 于 2022 年一季度发布。这项备受瞩目的标准旨在提供信息安全控制措施，修订后更符合技术进步、业务发展实践以及新法律和法规的要求。”

他补充道，2021 年很多其他方面的标准化工作也取得了进展，如：物联网安全和隐私、大数据安全和隐私、人工智能安全与隐私以及生物识别信息保护。除此之外，近期还发布了多个技术规范，包括提供智慧城市生态系统隐私保护指南的 ISO/IEC TS 27570，以及指导如何建立或完善强健网络系统来应对网络攻击的 ISO/IEC TS 27100。ISO/IEC 27000 系列标准及上述技术规范为建立和管理更安全的未来奠定了基础。