TECHNOLOGY WORKBOOK

[科技论坛 /TECH FORUM]

未雨绸缪，应对网络攻击

SECURITY BREACHES: ARE YOU READY?

Sean Hare, CAE, CGEIT
刘子亚 译，郭强 校

组织领导者如何应对网络安全挑战，关乎公司声誉。

网络安全是指运用工具和技术保障组织信息的可用性、完整性和保密性，它强调通过技术和网络协议建立多层防护和控制机制，来有效防止网络攻击和避免网络安全事件发生。尽管采取了多种积极防护措施，但各种形式的网络攻击仍层出不穷。鉴于这其中涉及巨大的经济利益，网络攻击还将持续升级。

网络犯罪不需要欺骗所有人，也不需要找到网络中的所有漏洞，只要找到一个切入点（某个人或某个漏洞）就够了。如果对网络犯罪妥协，你会面临丢失客户个人信息的风险。而且，在强调个人隐私权的今天，你可能会失去客户的信任，并使公司声誉受损。在风险如此大的情况下，当网络攻击发生时，组织是否已经做好准备?

这个问题不难回答，但如果组织不能未雨绸缪，很可能会陷入被动，进而可能导致公司的品牌及声誉受到重创。你需要制定计划、遴选团队成员，快速作出反应，从而妥善处理并成功化解威胁。其中，受托公司、法律和监管责任不只局限于

对抗网络攻击和控制相关损失。

负责任的组织需要制定明确的预防计划来尽可能地降低风险。不少公司提供欺诈预警和防身份信息窃取产品，但网络安全预防措施至少应包括以下内容：

1.合同和政策。确保集中放置、管理和保护组织与第三方签订的合同、公司政策和保单，因为法律顾问可能需要随时查阅。上述文件应定期发送给法律团队，确保法律团队存档最新信息。定期审计合同文件，并对其文字、日期和总体完整性进行审核。

2.第三方数据服务商。每年确认所有委托管理

公司数据的第三方服务商的系统和程序满足合规要求（如支付卡行业数据安全标准、SOC1/SOC2 审计等）。为实现最佳效能，第三方需要访问公司内部控制系统和数据中心，因此组织必须就这一需求在合同中做出明确规定。

3.安全测试。公司要定期进行安全测试，以确保运用了适当的最新网络安全措施并找到安全漏洞。这可以通过渗透测试和网络安全审计等形式进行管理，不过，建议这类工作交由独立的第三方执行，且各层测试都要有实测结果和改进建议。此外，还需第三方数据运营商提供相应的更新、审计和计划好的测试，以确保其能够满足极高的数据保护和网络安全标准。

4.培训。即使采用了最好的网络安全技术，人力仍是防范网络攻击的最佳保障。培训使人们具有安全意识，因此可能是最重要的手段。大多数网络攻击仅仅因某个人无意识地点击了一下鼠标而引发的。培训应包括网络犯罪的目标、详尽的注意事项、影响，以及员工在防范、发现和控制网络犯罪过程中的作用，还应涵盖一些网络基本知识，比如网络访问、电子邮件协议、密码更改的频次与强度，以及对系统访问的控制。培训必须全面、易于理解且行之有效。

网络攻击发生后的24小时尤为关键。一旦发现被攻击，必须立刻采取措施，以便损失可控。全球监管法规要求，在发现网络攻击事件72小时内，必须上报监管部门，同时告知其他受影响方。为确保组织为上述要求做好准备，可考虑采取以下步骤：

1.控制网络攻击。尽快隔断和遏制网络攻击。可能需要关闭并从网络中移走计算机、服务器和其他设备，甚至关闭整个网络。专门处理数据泄露问题的专业网络修复公司能协助快速保护公司的系统和网络，但这类公司大都要求提前签约。详细记录数据安全事件的日期和时间、发现攻击事件的人员、事件的性质、被窃取数据的类型，以及所有能够访问受影响系统的员工。

2.联系保险公司。降低风险最重要的一项投资，就是购买网络保险（cyber insurance）。因网络攻击事件联系保险公司时，需要简要告知对方事件情况与任何已知的风险敞口，便于对方备查。公司的保险代理可以就保险赔偿范围确认、可提供的支持服务以及可采取的必要措施等事项提供指导和支援，或者向你引荐其专门处理数据安全事件的法律顾问。如果公司尚未购买网络保险，强烈建议联系保险代理，详细了解保险覆盖范围。

3.联系法律顾问。法律顾问是处理网络攻击事件的另一关键资源，他们需要及时获得任何与事件相关的最新消息。作为隐私及合规领域专家，法律顾问将制定网络攻击事件的应对方案，确认诉讼及罚款风险；将就组织所做的任何沟通提供重要意见，并决定组织是否有必要告知受影响的个人和组织，包括顾客、供应商、媒体、发卡行、授权支付和处理公司及执法部门。法律顾问还要研究国内外法律、国际数据方面的法规及后续要求，确保履行所有受托责任。为保护组织及任何可能受到影响的个人，法律顾问将在与利益相关者的积极沟通发挥关键作用。此外，还处理客户的非现金补偿问题。

4.管理组织沟通。沟通在妥善处理数据泄露事件方面的重要性无须赘述。通过沟通，组织可以确立一个负责任的形象并体现出对受影响方的关注。所有的沟通都必须及时、透明和简洁，CEO、沟通/公共关系总监和法律顾问必须从一开始就紧密合作。不同的沟通渠道以及沟通对象必须要明确（比如客户、股东和董事会），在披露事件内容、企业所采取的措施以及存在的未决风险方面，所有声明应保持一致。公司的危机沟通计划应切合当上述需求，所有员工需将与此相关征询转交给沟通团队处理。

如今，沟通和商业发展都有赖于全球数据基础设施，而后者遭受的网络攻击司空见惯。尽管组织尽心竭力去保护数据资产，但仍无法规避攻击事件发生。公司如何应对与防范这类事件具有同等重要的意义，未雨绸缪、物尽其用、责任到位，将有助于公司及时响应、高效执行，并最终挽救公司的声誉。**SF**

Sean Hare, CAE，CGEIT，IMA信息技术和运营部门副总裁。联系方式：share@imanet.org。