

CISO 层面的指南：保护与第三方的连接

通过第三方识别风险

- 针对所有供应商关系和资产以及其中暴露的数据，制订并维持一份经过更新的清单。
- 审核各供应商或第三方可以访问的数据。确保本访问级别符合“最小特权”的原则。
- 基于泄露其系统将会对贵组织产生的影响评估您的供应商和第三方关系（低、中、高）。
- 从最高风险的供应商开始，评估各供应商的网络安全能力。符合相关标准是一个良好的出发点。为常规安全评估制订一个计划。您可能偶尔想对具有最高风险和/或对访问客户数据有最大权限供应商进行现场评估。

管理第三方安全

- 开展全面的尽职调查。在贵组织的征求建议书，与供应商签订的合同、业务连续性、事故响应和服务级别协议中明确网络安全预期。约定出现网络事件时的责任和义务。
 - 向您与其进行交易或分享数据的金融组织询问网络安全实践。对于贵组织必须遵守的任何网络安全要求，您的供应商和您与其分享数据或向其暴露资产的任何其他组织也必须遵守。
- 使用确定和约定的措施监测您的供应商遵守网络安全标准的情况。
- 与您的处理敏感数据的供应商核实，其是否为您在该供应商处开立的账户提供双因素验证、加密或其他安全措施。
- 确保您安装的所有第三方软件和硬件拥有安全握手协议，从而使启动程序通过认证码得到加密，如果不能识别代码将不予以执行。
- 如果您遇到假冒或不符合规格的供应商产品，可协商一个解决方案或者退出策略。
- 逐年评估供应商合同并确保它们持续符合您的战略方向和监管数据安全规定。合同终止后，包括将收回您资产或数据以及核实供应商已经将该资产或数据全部删除的规定，并撤销访问您系统或服务器的任何权限。

分享信息

- 确保您具有明确的沟通渠道和联系人，以便与贵组织的供应商和对手方沟通关于安全的问题。
- 与内部或外部利益相关者（包括金融领域内外的实体和公共机构）及时分享可靠、可操作的网络安全信息。
- 就威胁、薄弱环节、事故和响应而言，跟踪其他组织与其第三方经历的相关更新，以强化贵组织的防御，提高情景意识并扩大学习面。作为信息分享组织的组成部分，例如，金融服务信息共享分析中心（FS-ISAC）将促进更新。

如何在考虑网络安全的同时选择供应商

向潜在的供应商提出以下问题，以测试他们的网络准备状态和意识，以及对贵组织风险状况的影响：

- 他们有什么体验？查明该供应商服务客户的历史。它们以前是否服务过与贵组织类似的客户？
- 它们是否已记录符合已知网络安全标准的情况（例如 NIST 框架或者 ISO 27001），它们是否能提供 SOC2 报告？
- 要履行它们的服务，它们需要访问您的哪些数据和/或资产？它们是否要求明显不必要的访问权限？
- 它们怎样计划保护它们拥有的贵组织的资产和数据？
- 它们如何管理它们自身的第三方网络风险？它们是否能够提供有关它们的供应链的信息？
- 发生影响贵组织的资产和/或数据时，它们有哪些灾难恢复和业务连续性计划？
- 它们如何持续向贵组织提供更新？它们在其组织内部沟通趋势、威胁和变更的计划是什么？