网络安全与银行保密法 / 反洗钱

2016 年 10 月，美国金融犯罪执法局 (FinCEN) 就网络事件和网络犯罪问题向金融机构发布了指导文件，其中包括一些常见问题。

学习这份指南，了解可疑活动报告 (SAR) 必须包含哪些信息，成为金融机构在提交此类可疑活动报告时的一项非常重要的工作。下文将通过案例展示金融机构必须汇报的信息类型：[1]

来源和去向信息：

- IP 地址和端口信息，包含在世界标准时间中的相应日期时间戳
- 统一资源定位符 (URL) 地址
- 已知攻击向量
- 指令和控制节点

文件信息：

- 可能被恶意软件感染的文件的名称
- MD5、SHA-1 或 SHA-256 散列信息
- 电子邮件内容

主题用户名称：

- 与可疑活动相关的电子邮箱地址
- 与可疑活动相关的社交媒体帐号 / 昵称

系统更改：

- 系统注册信息更改
- 系统威胁指标
- 常见弱点和风险敞口

所涉帐户信息：

- 可能或实际受影响的帐户的信息
- 可能或实际参与的虚拟货币帐户（区分大小写）

从事网络安全工作的银行保密法 / 反洗钱专员通常是新手，或对该领域不甚了解。尽管行业趋势是银行保密法 / 反洗钱专员越来越有必要进一步学习和认识技术和网络威胁，但鉴于 10 月发布的指南，有必要安排银行保密法 / 反洗钱团队与机构的信息安全团队定期举行会议。

金融机构内部人员的交流非常关键。此外，银行保密法 / 反洗钱团队还有必要研究银行针对网络事件和网络犯罪制定的事故响应计划，制定银行保密法 / 反洗钱团队在事故处理流程中应当承担的责任。在事故处理环节纳入银行保密法 / 反洗钱团队有助于正确审查所有网络事件，确定是否需要创建可疑活动报告。追踪和审查网络案件非常重要，机构可借此识别可疑活动的常见模式和新趋势。为了解各个案件的关键共同点，机构可采用案

[1] “Frequently Asked Questions (FAQs) Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime and Cyber-Related Information through Suspicious Activity Reports (SARs)”，美国金融犯罪执法局，2016 年 10 月，https://www.fincen.gov/frequently-asked-questions-faqs-regarding-reporting-cyber-events-cyber-enabled-crime-and-cyber

件数据分析和整合工具。机构将深入分析结果报告给执法人员，有助于帮助他们综合各种关键信息，破获复杂的案件。在整个案件中，机构的金融机构工作人员很可能与执法人员合作，因此，规定机构应在何时创建可疑活动报告非常重要。机构是否应在调查结束时，掌握和归纳所有信息后即创建可疑报告？还是仅需在发现网络事件后的 60 天内创建？此外，金融机构工作人员如何判断一个网络事件是否需要上报？是在客户遭受损失后？金融机构遭受损失后？还是网络事件对客户造成重大影响后？美国金融犯罪执法局的指导意见是：“在确定某项网络事件是否需要上报时，金融机构应考虑所有关于该事件的已知信息，包括其性质及其针对的信息和系统。同样，在确定可疑交易涉及的金额时，金融机构应考虑该事件涉及或威胁的资金和资产总额。”

这些都是银行保密法 / 反洗钱团队和信息安全团队必须讨论的问题，进而确定机构的政策。做此决定时，机构必须记录做出的每项决定及其负责人。

机构在调查一项案件时，应努力搜集信息安全团队以及原本可能遭到网络攻击的客户所能提供的所有信息。一个有效的做法是制定案件搜集表，专门用于搜集网络事件的信息，从而指导信息安全团队攫取具体的相关信息，完成可疑活动报告。银行如果尽可能多地搜集信息，就能有效协助执法人员办案，并识别新的行业动向。

除了网络事故响应计划，机构还应完成的一项重要工作是，针对机构内的各项业务，制定银行保密法 / 反洗钱和欺诈事件响应计划。这些计划应相辅相成，并能整合成一个企业级风险事件和事故响应计划，与机构的业务连续性计划保持一致。

银行保密法 / 反洗钱事件响应计划应要求银行保密法 / 反洗钱团队处理和记录可能触发监管行动或罚款的网络及其他高风险事件和事故。

总之，所有银行保密法 / 反洗钱专员的一项重要工作是学习美国金融犯罪执法局的建议，与机构的信息安全团队合作，制定有效的计划，处理和报告可能有害的网络事件。一个有效的制度能够尽可能多地识别、收集和记录机构内潜在网络事件的相关信息。最后，机构最好与执法部门合作，向执法人员报告这些信息，以便他们更有效地办案和识别行业动向。

Joe Soniat，CAMS-FCI，Union Bank and Trust 副总裁兼银行保密法 / 反洗钱专员，美国弗吉尼亚州格伦阿林市，robert.soniat@bankatunion.com