# 网络安全威胁的种类

**AUTHOR** 作者

沈喆
Laurie Shen
Principal
总监

**lshen@uhy-us.com**
**212 381 4660**



无论在哪个行业，公司规模大小，网络攻击无疑会给每一个公司造成严重危害。它会导致公司声誉受损，业务受到重大干扰以及政府监管审查的增加。近期在金融服务行业发生的一些网络犯罪事件已经打击了消费者的信心，并使该行业的监管审查成为一个必要的手段。

为了制定一个全面的网络安全计划，首先我们需要确定的是网络安全威胁的种类。您看到的每个以网络安全漏洞为大标题的新闻事件基本上是这两种威胁中的一种：被动性威胁和侵略性威胁。

被动性的威胁是无声的数据收集行动。黑客通过这种无声的数据收集行动来收集有关消费者的数据，比如：支付卡的信息，个人身份的信息或敏感的专有信息，例如高频交易的算法解密、研究信息、高管会议纪要、交易流水账和风险模型。在头条新闻中我们越来越频繁地听到有关消费者数据被泄露的事情。对网络犯罪分子而言，专有信息数据的泄露往往给他们带来更可观的利润。

美国监管机构最近公布的一个涉及证券的案例是一个典型的被动性威胁的例子。2015年8月，监管机构宣布在全球范围内指控32人犯欺诈罪，他们是来自乌克兰的2个黑客及在俄罗斯、乌克兰、马耳他、塞勒斯，法国和美国的30个贸易商人。这两个黑客和这些商人利用从新闻专线服务途径获取的非公开机密信息非法获利1亿美元。此案导致了乌克兰境内的一家公司及其首席执行官同意支付3000万美金来和解指控。这起案件表明了全球范围的政府机构在一起协作打击网络犯罪分子。

侵略性的威胁往往严重干扰了企业业务的进行。这些干扰足以影响企业的关键系统。专有的数据也可能被摧毁或传播。 这些侵略性的威胁有它一定的目标，典型目标是那些管理关键基础设施的私营公司，比如铁路、机场、发电厂、水能源和电核处理设施。最近新闻里的一则案例是黑客在网上公布了客户信息。摩根士丹利在2015年1月报道，他们有大约35万名财富管理的客户记录被泄露了。导致这些信息泄露的起因是他们当时的投资经理把客户的信息下载转移到他自己在家里的电脑，而他的家用电脑被俄罗斯的黑客非法侵入并获取客户信息后在网上发布的。

# 如何制定有效的网络安全计划

## 1. 管理和风险评估

我们认为一个有效的网络安全程序必须从高层管理人员开始下达到每个基层员工，也就是要做到“上传下达”，在公司的最高管理层必须有这方面的强烈意识是非常关键的。网络安全应该设置在企业风险管理的程序中。我们通过对金融机构风险的组成部分：市场、信用、流动性、运营、财务、合规和声誉做综合审阅，网络安全显然影响着多个风险领域。此外，越来越多的董事会对网络安全工作开始发挥积极的影响和监督作用。除了利用公司内部的专业人员，董事会也应该有能力聘请外部的网络安全评估专家来对公司当前的风险控制措施做评估，并制定一个提高和完善的计划。网络安全质量的一个重要组成部分是对企业进行有效的网络安全风险评估，而且网络安全的风险评估应该定期进行，并与公司的产品、服务和地理位置结合起来。

## 2. 第三方与供应商管理

随着金融服务公司之间及其与供应商和金融市场之间在业务上产生越来越多的相互连接和系统数据的共享，对第三方的网络安全风险做评估已经是一个非常关键的确保自身网络安全的组成部分。此外，公司应该有一个有效的供应商管理计划，包括对新的供应商作尽职调查，持续的监测以及有关终止供应商的相应措施。

## 3. 培训和意识

在一个组织中最重要的防火墙是人类防火墙。公司应培训员工时刻准备反击各种网络和社交媒体的侵袭，比如如何识别和应对有目标性的网络钓鱼活动，电汇诈骗和欺骗攻击。公司也应不断对当前员工的培训和宣传措施的有效性做评估，并制定新的方案，以支持业务发展的需求，并针对企业最关心的领域提供专门的培训。培训应该每年进行，并以反复发生的事项为导向，在这些事项发生时进行培训，例如新员工入职、新的软件配置和采纳新的信息安全政策和程序。

## 4. 突发事件对策计划

根据金融监管机构的建议，企业应该指定一个中心化的事件对策团队来对公司现有对应突发事件的能力做评估，不断发现可以改进的机会，并开发可以满足业务要求的突发事件对策目标和计划。依赖于第三方服务提供商的企业需要一个衡量其供应商的相关网络安全风险的措施。总的来说，我们的目标是开发出可以有效管理网络安全风险的计划，提供内部控制的证据，以符合政府或行业规定的内控程序并且确保客户和供应商之间的一致性。




Our firm provides the information in this newsletter as tax information and general business or economic information or analysis for educational purposes, and none of the information contained herein is intended to serve as a solicitation of any service or product. This information does not constitute the provision of legal advice, tax advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisors. Before making any decision or taking any action, you should consult a professional advisor who has been provided with all pertinent facts relevant to your particular situation. Tax articles in this newsletter are not intended to be used, and cannot be used by any taxpayer, for the purpose of avoiding accuracy-related penalties that may be imposed on the taxpayer. The information is provided "as is," with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose.

UHY Advisors, Inc. provides tax and business consulting services through wholly owned subsidiary entities that operate under the name of "UHY Advisors." UHY Advisors, Inc. and its subsidiary entities are not licensed CPA firms. UHY LLP is a licensed independent CPA firm that performs attest services in an alternative practice structure with UHY Advisors, Inc. and its subsidiary entities. UHY Advisors, Inc. and UHY LLP are U.S. members of Urbach Hacker Young International Limited, a UK company, and form part of the international UHY network of legally independent accounting and consulting firms. "UHY" is the brand name for the UHY international network. Any services described herein are provided by UHY Advisors and/or UHY LLP (as the case may be) and not by UHY or any other member firm of UHY. Neither UHY nor any member of UHY has any liability for services provided by other members.