The attacks keep coming. In 2015 and 2016, a series of attacks were

made against banks using the SWIFT interbank payment system,

which handles trillions of dollars’ worth of transfers between 11,000

different financial institutions. In the most highly publicized incident,

hackers tried to steal $951 million from the Bangladesh Central

Bank account at the New York Federal Reserve. They succeeded

in stealing $101 million, some of which was recovered. Since then,

several other banks have been compromised, and multiple hacking

groups are now actively involved. In response, SWIFT has upgraded

its security protocols and issued new mandatory operational guidelines.

攻击还在继续。在2015年和2016年，针对使用SWIFT银行间支付系统的银行发生了一系列的攻击，该系统处理11000家金融机构间数万亿美元的转账业务。在最广为人知的事件中，黑客试图从孟加拉国中央银行在纽约联邦储备银行账户中窃取9.51亿美元。他们成功偷走了1.01亿美元，其中一部分后来被追回。从那时起，其他几家银行也受到了威胁，多个黑客团体现在也积极参与攻击。作为回应，SWIFT已升级它的安全协议，并发布了新的强制性操作指南。

In response to these and other attacks, regulators including the SEC

and FINRA and regulators in Europe have released updated cyber

security guidelines to ensure that financial firms take security risks

seriously. Their requirements extend out to partners and service

providers, including “law firms, accounting and marketing firms,

and even janitorial companies.

为了应对这些和其他攻击，包括SEC和FINRA在内的监管机构和欧洲监管机构都发布了最新的网络安全指南，以确保金融公司认真应对安全风险。他们的需求扩展到合作伙伴和服务供应商，包括“律师事务所、会计事务所和营销事务所，甚至是门卫公司。”