Security Threats to the Finance Industry

金融业的安全威胁

Cyber security and privacy are important to online ecommerce sites

like Etsy and Amazon (and, after then-candidate Obama’s handle

was hacked, to Twitter). But security is even more fundamentally

important to the financial services industry.

网络安全和隐私对在线电子商务网站很重要，如像Etsy和Amazon（然后，在当时还是总统候选人奥巴马的账号被黑客入侵后，就对Twitter来说也很重要了）。但安全对金融服务业来说具有更为根本的重要性。

Financial firms are obvious and constant targets for cyber criminals

—there is simply too much money and valuable customer data that

can be stolen. They are also targets for insider trading and financial

fraud; for cyber espionage and the theft of intellectual property; and

for hacktivists, terrorists, and nation state actors looking to disrupt a

country’s economic infrastructure through denial-of-service attacks

or more sophisticated integrity attacks.

金融公司是网络犯罪的明显和持续的目标-有太多的钱和宝贵的客户数据可以被盗取。它们也是内幕交易和金融欺诈的目标；网络间谍活动和知识产权盗窃；对黑客、恐怖分子和国家行动者想要通过拒绝服务攻击(DDOS)或者更复杂的完整性攻击来破坏一个国家的经济基础设施。

These threats are rapidly increasing as banks and trading firms open

up to the internet and mobile and other channels. The extensive

integration and interdependence of online financial systems provides

a massive attack surface.

随着银行和交易公司向互联网、移动端和其他渠道开放，这些威胁正在迅速地增加。在线金融系统之间广泛的的集成和相互依赖提供了巨大的攻击面。

For example, JP Morgan Chase, which *spends more than a quarter of*

*a billion dollars on its cyber security program each year*, was hacked

in June 2014 through a single unpatched server on the bank’s vast

network.7 An investigation involving the NSA, the FBI, federal prosecutors,

the Treasury Department, Homeland Security, and the Secret Service found that the hackers were inside JPMC’s systems for two months before being detected. The same hackers appear to have also attacked several other financial organizations.

例如，每年在网络安全项目上花费超过2.5亿美元的摩根大通(JPMC)，在2014年6月被黑客通过该银行大量服务器中地一台未打补丁地服务器入侵。一项由国家安全局、联邦调查局、联邦检察官、财政部、国土安全部和特勤处共同参与的调查发现黑客在被发现的前两个月就已经潜入JPMC的系统中。这些黑客似乎还攻击了其他几家金融机构。