Olga Zubenko, Daria Skvortsova
A.A. Martynenko, research supervisor
V.V. Gubkina, language adviser
SHEI "National Mining University", Dnipropetrovsk

Business Security Risk

When it comes to Business Security Risk, person who is not an IT specialist is likely to ask, "What is the risk?" Risk is the potential for loss and damage resulting in business impact. The comptroller of the currency discerns risk in four categories: operation risk, reputation risk, strategic risk and compliance risk.

Operation risk means the risk to earnings or capital on account of fails in the security processes or programs and people errors. Reputation risk threatens earnings or capital as a result of negative public opinion. Strategic risk is the risk to earnings or capital as a result of an unfavorable business decisions and lack of a proper response. Compliance risk is referred to infringement of the laws, prescribed practices, rules, policies and regulations of agreements and arrangements.

Hostile nation states. The Chinese are leaders in this category. China keeps their economy growing for compromising intellectual property.It has been joined to Operation Aurora where dozens of organizations were planed. Reuters recently released a report describing the threat posed by China. Many firms whose business revolves around intellectual property, namely tech firms, defense group companies, even Formula One teams complain that their systems are now under constant attack to extract proprietary information. Congress recently blocked scientific collaboration with China, citing high espionage risks.China increased international patent charges in 2010 by 56.2 percent, triple its 2006 figure.

Organized crime. Organized crime is known for compromising payment card numbers to commit fraud. Card data is becoming goods, with a drop in street value respectively. Steal of intellectual property is a growing tendency.

Insider. Insider threat goes beyond disconcerted employees. Authorized personnel may be willing to sell company secrets for profit such as the software developer that stole proprietary code. Insiders can also be tricked into disclosing sensitive information through social engineering.

Whistle-Blowing Sites. WikiLeaks is known for opening submissions of private media from anonymous sources.

For protection against a determined adversary it is important to establish Risk Management programs that meet compliance requirements. It is also suggested to adhere well-known practices to save business from negative impact. In addition to common practice, layered programs of control are proposed to protect data and important business processes, thus making priority protection to critical business services.