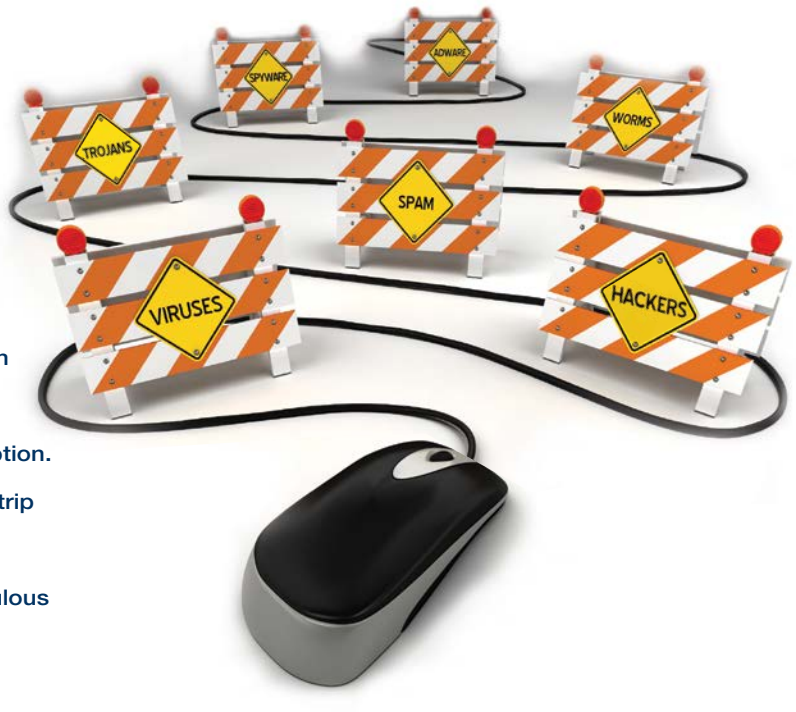
Endurance
YOUR RISK IS OUR FOCUS

ENDURANCE **INSURANCE**

Advanced Persistent Threats: New Concerns for Risk Managers

By Brad Gow
Senior Vice President, Endurance Pro
Email: bgow@enhinsurance.com



The risk management discipline always has contended with emerging threats to corporate balance sheets: from class action litigation to nanotechnology to supply chain interruption. Today, a new breed of sophisticated hacking attacks can strip companies of their most critical intellectual property and customer information, leaving them vulnerable to unscrupulous competitors and federal regulators.

Intellectual Property is a Cornerstone of Modern Business

The cost to develop or produce a new pharmaceutical, software operating system or Hollywood blockbuster can average hundreds of millions of dollars or more. Once this first pill or copy has been produced, it can be replicated for pennies. With so much future revenue tied to initial investments in research and development, the protection of intellectual property is critical. However, databases containing valuable information assets are now being systematically targeted by a hacking methodology known as the "Advanced Persistent Threat" (APT).

APTs are a particularly dangerous variant of computer hacking. 'Black hats' target individual organizations for an extended period of time and seek to map out internal networks, create trapdoors for later exploitation, and pilfer sensitive information and intellectual property. These predators are patient, deliberate, and often have access to substantial resources. Furthermore, the most dangerous black hats are offshore, out of the reach of federal authorities.

The Perpetrators of APTs Fall into a Number of Categories

Organized criminal gangs: Many are financed by the Russian Mafia and operate out of former Soviet states of Ukraine, Latvia and Estonia. These criminal enterprises are primarily motivated by money, looking to burrow into foreign corporate networks to steal credit card data and other sensitive information for sale in the black market. They are thought to be behind many of the most devastating privacy breach events.[1]

Politically motivated actors: In 2010, the devastating "Stuxnet" worm attack took a number of Iranian nuclear enrichment facilities offline (see sidebar). Based on the sophistication of the attack and the manner in which the Stuxnet Worm exploited weaknesses in Siemens' operating software, the attack was the result of years of patient effort targeting the centrifuges at these facilities.[2]

Nation states: These are arguably the most dangerous perpetrators and represent the greatest ongoing threat, responsible for the theft and transfer of billions of dollars in intellectual property annually. There is a great deal of information to suggest that hacking

Continued next page

This article is a reprint from the Spring 2012 Issue of The Edge newsletter.

[1] http://money.cnn.com/2011/07/27/technology/organized_cybercrime/index.htm
[2] http://blogs.mcafee.com/mcafee-labs/stuxnet-update; http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all

"Protecting corporate systems by employing the latest data encryption and intrusion protection technology, while necessary, comprises only one element of the layered protection that is required today to protect a corporate electronic information network."

U.S. corporate systems is tolerated if not sanctioned by the governments of China and Russia, with the intellectual property obtained from these attacks shared with companies close to those governments. These attacks focus on research-intensive industries, including aerospace, semiconductor, biotechnology and pharmaceuticals. Companies such as DuPont, Google, Northrop Grumman and Abbott Laboratories have been affected. In 2009 and 2010, energy companies, including Exxon Mobile Corporation, Royal Dutch Shell Plc, ConocoPhillips Inc. and BP plc, had oil exploration data and computerized topographical maps stolen by hackers believed to originate in China.[3]

What Risk Managers Can Do

With a mandate to focus on protecting a company's balance sheet risk against all threats, risk managers are no longer in a position to simply delegate the responsibility for APTs and other network-oriented threats to the Chief Information Officer. Protecting corporate systems by employing the latest data encryption and intrusion protection technology, while necessary, comprises only one element of the layered protection that is required today to protect a corporate electronic information network.

Risk managers would do well to work with their IT, Legal and HR colleagues to:

- ensure business partners, especially those providing critical network infrastructure such as cloud technology, maintain security standards at least on par with their internal requirements and vet them regularly;
- protect their organization by including liability and consequential damage provisions in their contracts with IT service providers, vendors, and others;
- limit insider threats by conducting detailed background checks for new employees, especially those in IT and operations functions, which would identify prior criminal hacking or identity theft activity; and
- obtain appropriate cyber insurance coverage for risk arising out of the theft or loss of customer information or the impact of network downtime as a result of malicious code or a hacking attack.

Technology has significantly increased the risks that organizations face today. With future revenues dependent on the security of data and intellectual property, the need for risk managers to focus on these digital assets is greater than ever. ◄

The Stuxnet Worm

In June, 2010, an extremely sophisticated and malicious code dubbed 'Stuxnet' was found buried deep in the operating systems of power plants and industrial networks around the world. Able to exploit the hardware and software used to control all manner of industrial systems and machinery, Stuxnet laid dormant until finding its ultimate target: centrifuges used for processing uranium in Iran's nuclear enrichment facilities. It is estimated that the worm effectively destroyed over 1,000 centrifuges in Iran's main Natanz facility and resulted in the suspension of Iran's nuclear materials processing operations. Although there is speculation as to who created the Stuxnet worm, its actual creators remain unknown. It is evident, however, that Stuxnet was developed by a team with millions of dollars at its disposal and with a mission that was purely political.

[3] http://www.bloomberg.com/news/2012-01-10/sec-push-may-yield-new-disclosures-of-cyber-attacks-on-companies. html; http://www.usatoday.com/tech/news/story/2011-11-03/china-russia-cybercrime/51064724/1