The cat and mouse game

by Ravi Das

As digital technology continues to transform the world of business, cybercrime continues to escalate, as these alarming figures for 2015 show:

- So far, there have been nearly 2,000,000 cases where malware infections were used in order to covertly steal money from private bank accounts.
- Almost 35% of servers have been affected by a major cyber-based attack.
- Cyberhackers used over 6.5 million unique hosts from which they launched their cyber-based attacks.
- The cybercriminals who wrote the actual malware code heavily targeted Adobe Flash Player.

Currently, the majority of cyberattacks are coming from Russia and China, and it seems that the Chinese hacker has the United States as its main prey. The reason why the Chinese cyberhacker has such an affinity towards US assets, is because the Chinese economy is growing, but not in a unilateral direction. Rather, it is trying to shift its entire economic structure from a labour-intensive, manufacturing-based one to a modern, cyber-based one similar to that of United States.

In order to make the Chinese economy on par with that of the United States, hackers – often instructed by their government – have no fear or qualms about launching these devastating attacks in order to steal what they need, without regard to the human or business impact of such an attack. The primary goal is gathering intelligence and even counterintelligence information. One of the best examples of this type of attack is the recent theft of over 22 million records from the US Office of Personnel Management.

What can be done to curtail these cyberattacks from China? Unfortunately, this is not an issue that can be solved easily or even quickly. It will take a mix of both technological and human efforts in order to make US assets safer not just from threats from China, but from other nations as well. Very large corporations and businesses must do their utmost to ensure that their servers and other types of intellectual property are well-protected from any outside threats. In terms of human effort this will be much trickier, mainly due to the threats faced by social engineering attacks. Essentially, this means using the tactics of manipulation and fear in order to get information and data out of key employees. As a result, the Chinese-based hacking groups have now shifted their efforts to conducting specialised social engineering attacks on both contractors and subcontractors. In turn, the Pentagon has tighter background checks in place on these employees, and if the organisations don't follow these policies, they could face very large fines and other penalties.

In sharp contrast, the European Union has taken much more proactive steps to fortify its borders. For example, the EU has recently implemented the Network and Information Security Directive (NISD). One of the primary goals of this directive is to help cultivate a much more coordinated approach in combating cyberthreats, as opposed to a singular and voluntary approach adopted by the United States. The NISD requires Member States:

- to craft and implement regulatory measures to achieve greater levels of cybersecurity from within their own infrastructure;
- to establish a well-regarded and authoritative or other policing body to monitor the implementations of the statutes of the NISD;
- to create the establishment of a Computer Emergency Response Team to handle security-related incidents and risks.

The US Government needs to take a much more proactive mindset in protecting its assets and borders. With a new political administration soon to be in place, perhaps this will now happen. In the end, it will take the utmost of human vigilance for the American mouse to stop being the prey for the Chinese cat.