IMF cyber attack boosts calls for global action

LONDON (Reuters) - Governments, multinational corporations and global institutions are losing the battle against computer hackers and must combine their resources if they are to lock out cyber intruders, experts say.

The International Monetary Fund has joined Sony and Google on a growing list of hacking victims but it is hard to identify the culprits who consistently manage to keep one technological step ahead of their pursuers.

"This is an example of technology developing faster than the frameworks and sometimes the regulations around that," said Unilever chief executive Paul Polman on the sidelines of a World Economic Forum meeting in Jakarta.

Cyber security experts say the only way to effectively combat the menace is for the public and private sectors to join forces and combine greater regulation with international action.

"Clearly we are losing the battle," said Vijay Mukhi, one of India's leading cyber security experts.

"We are not doing enough... every year we hope things will change but now people like me have turned cynical. It requires co-operation on a global scale," he said.

Earlier this month, Internet giant Google pointed the finger at Chinese hackers for an attempt to access the Gmail accounts of assorted rights activists, officials and others.

Entertainment giant Sony suffered serious damage to its reputation after hackers accessed the details of thousands of PlayStation users, while Lockheed Martin and Citi also reported attempts to steal data.

The growing complexity and seriousness of cyber attacks has begun to break down some of the stigma of being a victim, firms, government and organisations realizing they must work together.

"There has been a real change," said John Bassett, senior fellow for cyber security at London's Royal United Services Institute and a former senior official at Britain's signals intelligence agency GCHQ.

"There is much more awareness of the threat (and) organisations are being much more open about the attacks they face. Lockheed, Google and now the IMF are showing far more openness than organisations would have done a year ago."

"NAME AND SHAME"

Experts like Alexander Klimburg, said the attempt to steal sensitive information from the IMF, the global lender of last resort, was a chance for all sides to come together to confront a common menace.

"This is potentially a great opportunity to launch a "communal" investigation into an attack on a "communal" institution," said Klimburg, a cyber security specialist at the Austrian Institute for International Affairs.

"If fingers can be pointed, they should be pointed. The only way to stop such attacks is 'naming and shaming', and in this case, unlike those of individual national governments, there is a clear global interest at stake."

With the volume of data stored online increasing exponentially every year, some specialists say the problem is escalating out of control and action must be taken.

While some civil liberties campaigners fear giving governments greater control of the Internet would undermine privacy, others say that same privacy is already being undermined by both criminal and state-linked hackers.

STUXNET - SHAPE OF THINGS TO COME?

Countries such as the United States have begun to publish national doctrines on cyber security and warfare but talks on international standards and agreements seem remote.

In reality, most states engage in some form of electronic espionage but some worry it is now getting out of control.

The Stuxnet computer worm widely believed to have been built by a state intelligence agency to attack the Iranian nuclear program through reprogramming centrifuges to inflict damage on themselves is seen by some as a sign of things to come.

Both Western and emerging powers have plowed funding into cyber warfare capabilities, with China, Russia and smaller states believed to see it as an area in which they can challenge the conventional military superiority of the United States.

As Chinese and Vietnamese hackers apparently attack systems in each other's countries as tensions over a disputed maritime border escalate, there are also growing worries about the potential risks of damaging state-on-state cyber warfare.

Although he did not mention China by name, Vietnam's Prime Minister Nguyen Tan Dung on Monday announced a directive ordering government agencies to boost cyber security and increase research on prevention of cyber war.

"Many serious threats have emerged that seriously endanger the application of digital technology for socio-economic development and ensuring national defense and security," the directive said.

Even if international agreement were reached on a common approach, investigators face almost insurmountable technical difficulties in tracing the source of a cyber attack.

"Such attacks are very difficult to pinpoint and so responding is both difficult and dangerous as wrong reactions can cause international tensions," said Tony Dyhouse, cybersecurity director at the UK-based Digital Systems Knowledge Transfer Network.

(Additional reporting by Reuters bureau; Editing by Jon Boyle)