

**PRESS RELEASE: 29.09.11****The Considerable Cost of Hacking****Written by Verity Sleeman, Comment by Varun Uppal**

Viktor Pleshchuk witnessed two of his properties and his two cars - a Lada and BMW - auctioned off in Saint Petersburg on Monday.

But then again, if you are going to steal £9m from RBS and hack in to steal thousands of people's personal data - that's the price you pay when you get caught!

Despite the personal consequences of Pleshchuk's actions grabbing most of the headlines, a more obvious concern - the aftermath inflicted on company's reputations and finances - seems to have slipped under the media radar.

Varun Uppal, a Technical Consultant at Information Risk Management Plc (IRM) outlined the costs encountered by companies after an online security breach. He said:

"Costs can vary significantly but it goes without saying there are always considerable monetary implications following attacks of this scale."

"Cost bearing measures include beefing up internal security technology and processes, hiring forensic investigators, legal fees, PR costs and possible reimbursements to customers. All of this can result in a hefty bill to the tune of a few million."

Once a company suffers a security breach, simply blocking access to the offending party and returning a company website and datasheets to their previous form is unfortunately not nearly enough in terms of corrective action.

Uppal outlined the basic steps breached companies should take:

"Damage control is a shared responsibility - every business department involved has to work in parallel, as it could be any level or function within the business that could identify where an incident began."

"Once the severity level has been ascertained, the incident response process needs to come into action, with external technological support or an internal security team increasing monitoring practices and working to contain the incident."

"Collectively the company needs to prioritise the matter to senior management/board level, in order that tough business decisions can be made quickly. Management then needs to get the PR ball rolling - so that they are on hand to pacify shareholder and customer concerns."

"In addition to this, the Legal Department needs to be informed for the same external reputation purpose - court filings, subpoenas or warrants may need to be raised."

But what of the perpetrator? Computer hackers are becoming increasingly annoying to large companies. And ironically, the highly destructive and intricate crimes are committed by young men and women yet to get a real/normal/regular job, and typically belong to organisations such as Anonymous and LulzSec.



Uppal explains that being able to track a hacker depends on the clues that he/she has left behind.

He said, "Tracking methods usually start with identifying trails left behind and attempting to recreate steps taken by perpetrators. Internal response teams or external consultants perform forensic analysis on systems deemed to have been compromised – to try and identify the attacker's actions."

"If the forensic investigation exposes concrete information about the possible identity or source of an attack - the affected party can use this information to formally file a case in their local jurisdiction, or the jurisdiction where the attack originated from, provided an extradition treaty exists."

"As you can appreciate - the Internet offers a high level of anonymity and clever perpetrators can leverage this to cover their tracks, thereby making it very difficult to identify the source of an attack. However, sometimes a single piece of evidence can give away a lot to investigators, which appears to have been the case with Viktor Pleshchuk."

Even though it is reassuring that the physical evidence left behind in a robbery used to convict criminals has an online/virtual counterpart/equivalent, the regularity of security breaches suggest this relatively new wave of criminality has not yet peaked.

ENDS

Notes to Editors

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy with 13 years experience working with large enterprises, helping our clients identify and mitigate the risks inherent in today's increasingly interconnected business environments.

Today our portfolio includes a wide range of technical assurance services, complemented with a wealth of security management and risk assessment options, covering the full spectrum of our clients' information security requirements.

For further information, please contact IRM on:

Tel: +44 (0)20 7808 6420

Email: press@irmplc.com

Website: www.irmplc.com

Twitter: #IRM_tweet