S. RAJARATNAM SCHOOL
OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

RSIS COMMENTARIES

No. 177/2013 dated 27 September 2013

Enhancing Cybersecurity & Data Privacy: The Role of Private Citizens

By Caitríona H. Heinl

Synopsis

Cybersecurity is increasingly being enhanced worldwide. At the same time, it is equally necessary to be mindful of civil liberties and data privacy protections. Initiatives which co-opt citizens can be effective in achieving these goals.

Commentary

AS GOVERNMENTS and public authorities develop and implement cybersecurity measures, it is essential that civil liberties such as data privacy and data protection be respected. Where possible, both security and data privacy principles should be incorporated from the outset in such measures - in other words by design.

Consequently, novel initiatives which strengthen cybersecurity and data privacy as well as increase public awareness of their importance should be encouraged since citizens' buy-in, loyalty and cooperation are essential for effective cybersecurity strategies. Furthermore, while the end-user is often identified as the weakest link in terms of cybersecurity, he can also be the most valuable link if novel strategies are applied.

Co-ownership of responsibility for cybersecurity

There are five key considerations underlying initiatives which co-opt citizens for enhancing cybersecurity. First, for much-needed cybersecurity measures to be effective when implemented they must respect fundamental rights and protect civil liberties such as data privacy and data protection. Deviation from these principles will only undermine the credibility of authorities and impede the effectiveness of the measures.

Second, awareness-raising initiatives and constructive debate are essential to ensure citizens are fully informed and aware about the issues and risks they encounter on a daily basis in their use of ICT as well as their own role in ensuring cybersecurity.

Third, citizens should be made aware that they have a shared responsibility for cybersecurity and data privacy. As end-users, individual citizens must be made to realise that they too play a crucial role and that there is a shared responsibility for cybersecurity and data privacy between public authorities, the private sector and individuals as the end-user.

Fourth, recent initiatives to stimulate the creation of innovative and useful tools can assist public authorities and

companies identify much-needed talent. Lastly, most initiatives are easily transferable and may therefore be adopted or tweaked at local, national or international level.

A toolbox of initiatives

Several examples of recent initiatives and developments support these principles. They include outreach campaigns to promote public awareness through education, cybersecurity months, transparency reports such as the release for the first time on 27 August 2013 of Facebook's Global Government Requests Report, and hackathons like this year's "EUhackathon 2013".

The Facebook report details, for purposes of increased transparency and trust, which countries requested information about Facebook users, the number of requests and number of user accounts specified in those requests, and the percentage of requests in which the company was legally obliged to disclose some data.

EUhackathon 2013, themed *"hACK4YOUrRIGhTS"*, was a 24-hour coding session held in September 2013 in Google's Brussels offices. It focused on raising awareness of government requests to companies for user information and the "empower[ing] of citizens to stand up for their fundamental rights" through the creation of tools to be made freely available online by citizens for citizens to know when and why governments demand access to their information.

Selected teams of coders, developers and hackers were challenged to create applications on the state of government surveillance by using data sets from network analysis, corporate transparency reports, government reports, and Freedom of Information Requests.

While such initiatives are significant and should be further encouraged, there is still, however, an urgent need for more of these kinds of initiatives which should be broader in their scope.

Solving complex cybersecurity dilemmas

Open innovation challenges allow public authorities, corporations or even civil society groups to tailor a cost-effective challenge for citizens by placing a specific question on online innovation forums. A challenge may be limited to national applicants or it may be opened to the wider global community and should therefore be considered as a possible solution for finding new policy or theoretical concepts and novel technological tools.

For instance, the online community could be asked in an open cybersecurity challenge, "how can big data be best leveraged to enhance cybersecurity while ensuring data privacy?" The parameters may be set so that solutions must incorporate principles of security and data privacy by design. For example, open innovation challenges were launched earlier this year on pre-existing innovation forums by USAID and the Humanity United Foundation to find a mechanism for secure communications during a crisis. In July 2013 the US Department of State launched the *2013 Innovation in Arms Control Challenge* for a prize of US$10,000 to find out "what information technology tools and concepts can support future arms control inspections".

Results can often be quite surprising, as can the sources of submissions - winners of one challenge included a student, a scientist, and a defence industry consultant. It is therefore worth considering the feasibility of open innovation challenges for enhancing cybersecurity and civil liberties protections since they are solutions-based in nature, stimulate innovation, are relatively cost-effective, and enhance awareness of the issues.

Furthermore, co-ownership of responsibility is encouraged since citizens are engaged to co-produce exciting and novel solutions for burning policy and technological questions. In short, an open cybersecurity challenge could quite easily provide a valuable and simple opportunity for solving some of the most complex cybersecurity and related data privacy problems.

Caitríona H. Heinl is a Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.