SOCIAL CYBER INSTITUTE

Cyber incompetence is killing more people than cyber attacks; and costing us more

New Report by a Research Start-up

6 October 2019

Cyber incompetence will kill more people than cyber attacks. That's the departure point of a new report from the Social Cyber Institute by two prominent Australian professors.

346 people were killed in two separate crashes of Boeing 737 Max because of mismanagement of software. The company has incurred US$5.6 billion in losses related to the aircraft. Boeing says it is working very closely on new certification of the 737 MAX software update.

In addition to fatalities in aircraft, hospitals and in automobiles from computer error, the economic costs of managing software's power and pitfalls are now often at or around the billion dollar mark: US$5 billion for Facebook and US$500 million for Australia's Commonwealth Bank. These losses are higher than those now being incurred by breaches in the worst cyber attacks for individual companies.

Security in cyber space has already migrated well beyond the technical sphere.

"No-one is tracking the number of deaths caused by computer error in hospitals and on our roads, much less framing a comprehensive policy response", according to report co-author Professor Greg Austin. "Behind each death by computer error is a human mistake, usually caused by faults in management of the cyber ecosystem."

"To begin to address the social aspects of human security in cyber space, we need a new concept of 'social cyber value'", according to Professor Glenn Withers, immediate Past President of the Academy of Social Sciences of Australia. "We have to recognise human use and misuse of relevant technology as central."

The idea of "creating social cyber value" is based on management integration of several related problem sets in cyber space: incompetence, insecurity, disinformation, slow digital transformation, and ethical insensitivity.

All countries need a human capital policy for cyber space. Israel is one of the few countries that has one.

The report based on a year-long research effort and a detailed paper by the two co-authors, validated in part by a March 2019 report from the US National Academies for the US intelligence community that calls for a new focus on social cyber security. The authors call for a radical shake-up in organisational structures to place CSOs and CISOs under a new post responsible for all aspects of information technology, especially human capital and social aspects. Will countries need a Bureau of Software Safety to prevent spiralling numbers of deaths by computer error?

For information on the Social Cyber Group, see www.socialcyber.co.

Enquiries:
Business and Media: Lisa Materano +61 (0)438134558
Research Institute Academic Director: Glenn Withers +61 (0)416249350
Research Adviser: Greg Austin +61 (0)450190323