Institution:
University of Cambridge

Unit of Assessment:
UoA11

Title of case study:
Security Economics

1. Summary of the impact (indicative maximum 100 words)

Professor Ross Anderson's (University of Cambridge) research in security economics has had considerable impact on public policy and industry practice. Through two reports for ENISA, his work has directly influenced *European Commission* policy on combatting cyber-crime and on protecting the internet infrastructure. Through his membership of a Blackett Review and appearances before parliamentary committees, he has influenced *UK government policy* on cyber-security. Personally, and through the positions to which members his research team have moved, his research has influenced a range of organisations, including the *US government*, the *European Union*, *Google*, and *Microsoft*.

2. Underpinning research (indicative maximum 500 words)

Security economics is central to understanding cyber-security and to making policy decisions affected by it. It considers *human behaviour*, particularly *incentives*, as a vital part of any security system. As large systems increasingly involve many diverse stakeholders, security depends on the self-interested behaviour of participants who may be competitors. To ensure security, and dependability in general, engineers and policymakers must devise rules and incentives that lead participants to behave in ways such that the resulting equilibrium is sustainable.

While writing his book "Security Engineering" in the late 1990s, Professor Anderson (Lecturer from 1995, Reader from 2000, Professor from 2003 to present) noticed that most of his case histories had significant considerations of economic incentive as well as traditional systems engineering. The economic research from the book became a paper "Why Information Security is Hard – An Economic Perspective" [1]. Both book and paper are widely cited. Their publication sparked interest in the subject leading to the first workshop in the field, in 2002, organised by Anderson himself. Since then Anderson's research group has published numerous papers, applying the economic analysis of incentives to a wide range of security problems.

The initial research explained, in qualitative terms, why many information goods and services are insecure: the combination of network externalities, low marginal costs and technical lock-in makes the computer industry prone to monopolies. For example, during market races, companies leave systems open to appeal to complementers, but later they secure them in ways designed to maximise customer lock-in. As a second example, security products are often a "lemons market": for example, few users can tell the difference between a good antivirus program and a bad one.

Later research (early 2000s) investigated the circumstances in which open-source software might be more secure than proprietary products; the likely effect on competition of adding hardware TPM security devices to PCs; the initial costs versus the maintenance costs of security systems; and market failure in certification systems. Work directed at particular applications included the economics of censorship resistance [2], the economics of location privacy, and the security economics of smart meters [3].

A further research topic (2005 onwards) has been the econometrics of online and electronic crime [4]. Anderson and his research team have built systems to monitor malware, spam and phishing, and worked with organisations with access to masses of data, including Google, Yahoo, and Microsoft.

The final strand of Anderson's research is policy, bringing together the theory and the data to advise governments on issues such as breach disclosure laws, software liability, and budgetary priorities. The work continues today. For example, 2012 saw a major report on the economics of cybercrime at the request of the Chief Scientific Adviser at the Ministry of Defence [5], while January 2013 saw the start of a major collaboration, funded by the US Department of Homeland Security, between Cambridge, CMU, SMU and the US National Cyber Forensics Training Alliance (which includes the FBI and the Secret Service).

The Cambridge researchers involved were Ross Anderson (permanent academic staff since 1992), Richard Clayton (post-doc, since 2005), Tyler Moore (PhD student, 2004–8; Harvard 2008–12; now at Southern Methodist University), Andy Ozment (PhD student, 2004–8; now at the White House), George Danezis (post-doc, 2004–5; at Microsoft Research since 2007); Shishir Nagaraja (PhD student, 2004–8, then UIUC, IIIT, and Birmingham); Joe Bonneau (PhD student, 2008–12; now at Google) and Sören Preibusch (PhD student, 2008–12, now at Microsoft Research).

3. References to the research (indicative maximum of six references)

*Indicates those references most representative of the quality of the research.

*[1]. 'Why Information Security is Hard -- An Economic Perspective', Ross Anderson, in *Proceedings of the 17th Computer Security Applications Conference*, IEEE Computer Society Press (2001), ISBN 0-7695-1405-7, pp 358–365; also given as a distinguished lecture at the Symposium on Operating Systems Principles, Banff, October 2001.
DOI: http://dx.doi.org/10.1109/ACSAC.2001.991552

*[2]. Danezis, George, and Ross Anderson. "The economics of censorship resistance." *Proceedings of the 3rd Annual Workshop on Economics and Information Security* (WEIS04), 2004.
PDF: http://www.cl.cam.ac.uk/~rja14/Papers/redblue.pdf
Re-published as Danezis, George, and Ross Anderson. "The economics of resisting censorship." *IEEE Security & Privacy* **3**(1):45-50 (2005).
DOI: http://dx.doi.org/10.1109/MSP.2005.29

[3]. Anderson, Ross, and Shailendra Fuloria. "On the Security Economics of Electricity Metering." *Proceedings of the 9th Annual Workshop on Economics and Information Security* (WEIS 2010).
PDF: http://www.cl.cam.ac.uk/~rja14/Papers/meters-weis.pdf

*[4]. 'The Economics of Online Crime', Tyler Moore, Richard Clayton and Ross Anderson, in *Journal of Economic Perspectives* **23**(3):3–20 (2009).
DOI: http://dx.doi.org/10.1257/jep.23.3.3

[5]. 'Measuring the Cost of Cybercrime', Ross Anderson, Chris Barton, Rainer Böhme. Richard Clayton, Michel van Eeten, Michael Levi, Tyler Moore and Stefan Savage, *Proceedings of the 11th Annual Workshop on the Economics of Information Security* (WEIS 2012).
http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

4. Details of the impact (indicative maximum 750 words)

The principal impact of this research has been on public policy. Anderson's election to the Royal Society, in 2009, was a direct consequence of the impact of his research and his influence in the field:

"*He is also one of the founders of the study of information security economics, which not only illuminates where the most effective attacks and defences may be found, but is also of fundamental importance to making policy for the information society*."
Royal Society Election Citation.

European Commission

Anderson and colleagues have directly influenced the implemented policy of the European Commission. They produced two major reports for the European Network and Information Security Agency (ENISA): the first (2008) on consumer and single-market aspects [6] and the second (2011) on protecting the Internet infrastructure [7]. Many of the recommendations from the 2008 report [6] are being implemented, including uniform fraud reporting across Europe (implemented from 2012 in the Eurozone), security breach disclosure laws (done in telecoms, under way for other sectors as part of the Data Protection Regulation) and better international police collaboration (with extra cybercrime staff for Europol)[12].

"*Prof Anderson's early research on security economics as well as the two studies he has carried out for ENISA have been very inspirational for the development of EC's regulatory and policy proposals to ensure transparency and accountability in the provisioning security of electronic communication services."* [12]

The 2011 report [7] has been adopted as policy *in its entirety* by ENISA and thus by the European Commission.

UK Government

Anderson has directly informed the public policy debate in the UK. He is frequently asked to testify before parliamentary committees and to advise EU policy working groups. For example, he has testified in person at Westminster to the Commons Select Committee on Scientific Advice and Evidence in Emergencies (17 November 2010):

*"As we began our inquiry, the "Stuxnet" worm had just been identified to be circulating… We were told that it would have taken six people to create the worm over five months, with funding to the order of £1 million.**[cites Anderson's evidence]"*** [8]

and to the Joint Select Committee on the Draft Communications Data Bill (4 September 2012):

"*Prof. Anderson's evidence was key to the Committee reaching its conclusions and in its subsequent opposition to the Bill. We were particularly struck and influenced by the novel approach of considering the economic incentives faced by those securing and attacking digital services."* [9]

In 2010, Anderson was invited, by the Government Chief Scientific Adviser, to join the Blackett Review of Cybersecurity, which fed into the National Security Strategy [10], which in turn led to the cabinet approving an extra £640m budget for cybersecurity over 2011–5:

"*Ross's input occurred at a key point in the development of the Government's Cyber security programme… The output of the Blackett Review meetings was very influential across a number of the programme work streams in supporting that programme, and Ross's work on security economics was a key contributor to this"* [11]

The Chief Scientific Adviser at the Ministry of Defence asked the Cambridge team to produce a report on the costs of cybercrime, which was published in 2012 [5].

RCUK's green paper for cybersecurity research in June 2011 identified nine themes. Two were directly in security economics ("Deployment, economics, motivation and regulation of cyber security measures" and "cybercrime"), another in the related and derivative field of the behavioural economics of security ("human factors and useable security"), and another spanning both ("Global threats, 'cyberwar', ethics, regulation, policy and legality"). The first two themes grew out of Anderson's original research while the other two have been strongly influenced by it.

Wider impacts

Anderson has been a visiting scientist at Google, while his students and postdocs have interned at Yahoo, Microsoft, Easynet and Scottish Telecom. Four of Anderson's former students now work in relevant government or industry posts: the White House (Ozment), Google (Bonneau), Microsoft Research (Danezis, Preibusch).

5. Sources to corroborate the impact (indicative maximum of 10 references)

[6]. *Security Economics and the Internal Market,* Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, published by the European Network and Information Security Agency, March 2008; short versions published as 'Security Economics and European Policy' in *Workshop on the Economics of Information Security* (WEIS 08) and in ISSE 2008.
ENISA website: http://www.enisa.europa.eu/publications/archive/economics-sec
DOI (of short version): http://dx.doi.org/10.1007/978-0-387-09762-6_3

[7]. *Resilience of the Internet Interconnection Ecosystem*, Panagiotis Trimintzios, Chris Hall, Richard Clayton, Evangelos Ouzounis and Ross Anderson, European Network and Information Security Agency, April 2011; abridged version published at the *Workshop on the Economics of Information Security*, 2011.
ENISA website: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report
DOI (of abridged version): http://dx.doi.org/10.1007/978-1-4614-1981-5_6

[8] Commons Select Committee on Scientific Advice and Evidence in Emergencies (Anderson gave oral evidence on 17 November 2010)

http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2010/scientific-advice-in-emergencies/

[9] Joint Select Committee on the Draft Communications Data Bill
(Anderson gave oral evidence on 4 September 2012)
http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/communications-data-bill-further-informantion-page/

[10] Letter from member Joint Select Committee on the Draft Communications Data Bill

[11] Letter from Assistant Director, Department for Business

[12] Letter from Head, Task Force Legislation Team, Directorate General for Communications Networks, Content and Technology