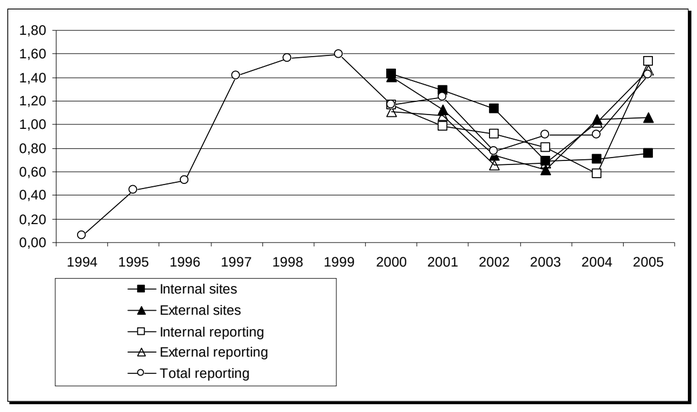
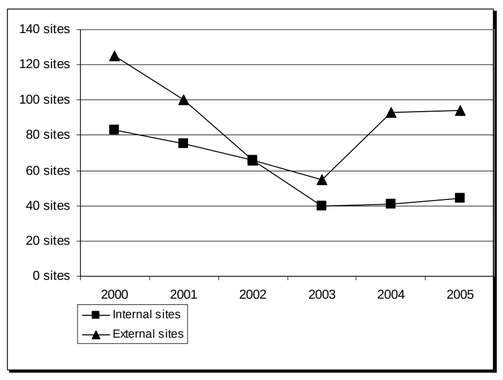
Preserving a balanced CSIRT constituency

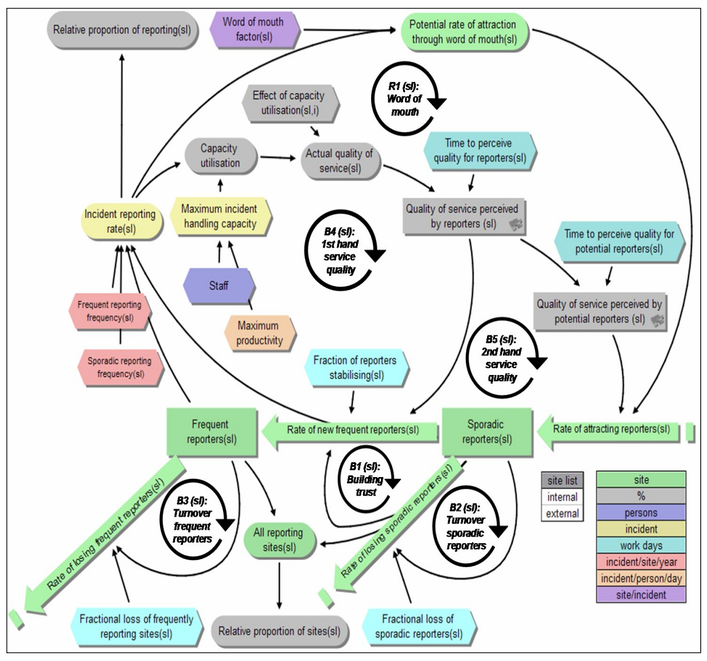
- Goal: Improve retaining the internal constituency – i.e., the customer base or community who by its funding enable the existence of the CSIRT.
- CSIRT = Computer Security Incident Team
- How: Workshops, face-to-face meetings, frequent teleconferences & virtual meetings with managing director and staff of CSIRT.
- Access to numerical data, docs and mental models
- Partner: One of Europe's largest and oldest coordinating CSIRTs



Historical variation relative to average for internal and external reporting sites as well as internal and external reporting in 2000-2005, and for total high-priority incident reporting 1994-2005

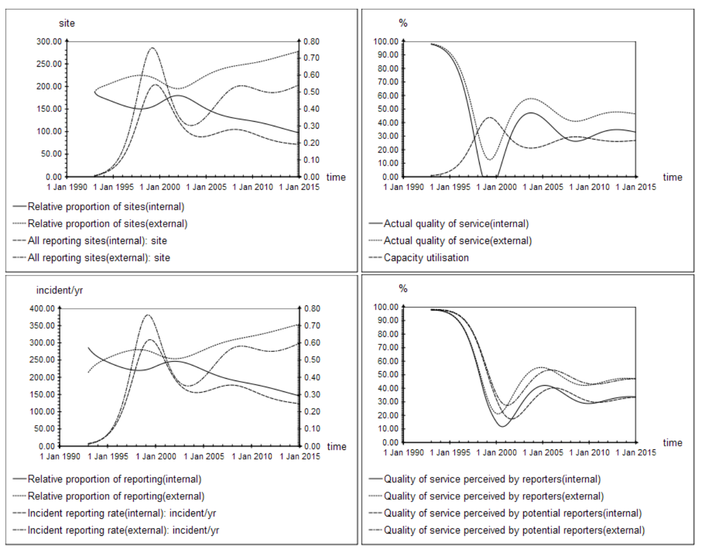


The number of sites varies with a similar pattern as the total number of incidents reported. However, the internal sites seems to vary more in absolute numbers, and an increasing gap in the number of reporting sites is emerging from 2003.

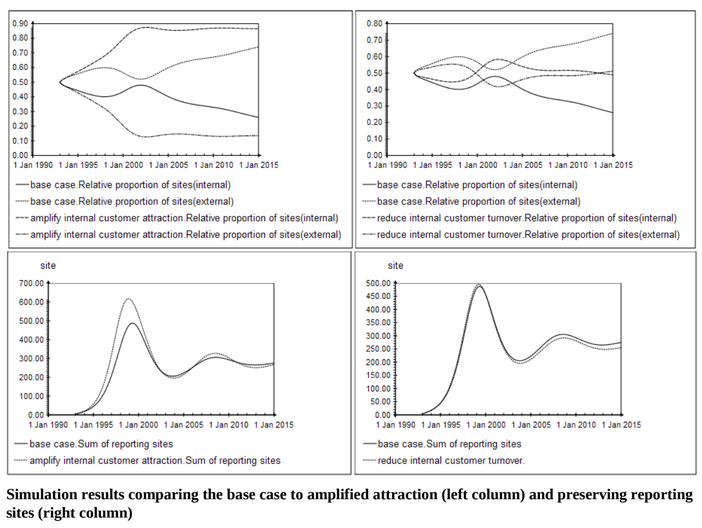


The handling capacity represents an internal limit to the growth of the CSIRTs workload and this forms several balancing feedback loops that may counteract growth of sites by slowing down the rate of attraction of new sites, B5 (sl) and the rate of new frequent reporters through B4 (sl)

CSIRTs get incident reports from their constituency (internal sites) and from external sites that detect incidents coming from the CSIRTs constituency. The observed increasing reliance on external reporting is a problem, since it indicates that the recognition of the CSIRT by its constituency is correspondingly weaker. It also means that external reporting fills up more of the incident response capacity.



The base case scenario shows the behavior of key variables from 1993 to 2015, using the historical policies identified in the case



Simulation results comparing the base case to amplified attraction (left column) and preserving reporting sites (right column)

Base Run (l.h.s.): The instabilities create an imbalance that – if it persists – could threaten the very existence of the CSIRT.

Policy analysis (r.h.s.): A strategy that reduces the turnover of the most frequent reporters (right) is much better than attempting to attract a higher number of frequent reporters (left)

Johannes Wiik[1], Jose J. Gonzalez[2], Pål I. Davidsen[3], Klaus-Peter Kossakowski[4]
[1]University of Agder, Faculty of Engineering and Science, Department of ICT, 4898 Grimstad, Norway
[2]University of Agder, Faculty of Engineering and Science, Department of ICT, 4898 Grimstad, Norway
[2]NISlab, Gjøvik University College, 2802 Gjøvik, Norway
[3]Institute for geography, University of Bergen, 5020 Bergen, Norway
[4]SEI Europe, Carnegie Mellon University, 60 322 Frankfurt, Germany

UNIVERSITY OF AGDER