Overview

1. Context and problem
2. Research approach
3. Simulation model structure
4. Management strategies
5. Conclusion
Context

- The study is based on a coordinating CSIRT
- Only high priority incidents are considered
- Low priority incidents such as port scans and spam complaints have been ignored.
- Manual reports come from both inside and outside the constituency of the CSIRT

A dynamic problem

Problem:
- What are the causes behind these dynamics?
- What are the implications relative to the CSIRT mission?
- How will various policies influence the system and the mission over time in the future?
Overview

1. Context and problem
2. Research approach
3. Simulation model structure
4. Management strategies
5. Conclusion

Approach:
Build a simulation model of the real case

Real World Case
- system behaviour
- system structure

Simulated World/Controlled Environment
- simulated behaviour
- simulation model structure

1. improved mental models
2. new goals
3. better policies

1. mental models
2. written information
3. numerical data
Overview

1. Context and problem
2. Research approach
3. Simulation model structure
4. Management strategies
5. Conclusion

Quick intro to system dynamics concepts

[Diagram of stock and flow with feedback loops and delay mark]
Reporting sites enter and leave

The growth process:
Word of mouth (Reinforcing feedback)

Variation in sites and reporting

Word of mouth factor
Potential rate of attraction through word of mouth

Art: Word of mouth

Word of mouth

Reporting sites

Frequent reporting sites

Sparsodic reporting sites

All reporting sites

Variation in sites

and reporting

Reporting sites enter and leave

Word of mouth factor

Potential rate of attraction through word of mouth
Overview

1. Context and problem
2. Research approach
3. Simulation model structure
4. Management strategies
5. Conclusion
Base case 1993-2015

Note:
This is a replication of behaviour patterns only.
The exact numbers are not comparable to historical data.

Behaviour generated from the structure:
S-shaped growth (or decline) followed by damped oscillations

Base case continued:
Perceived versus actual quality of service

Notice:
• Perceived quality is smoother and delayed compared to the actual quality
• Important to understand overshoot and oscillations
A new goal: Stable balance

What-if 1: We double the staff
What-if 1: We double the staff?

1. No change in behaviour pattern
2. The system adjusts to the new situation, but the problem persists (and gets slightly worse)
3. A fix that fails! Counterintuitive?
What-if 2:
We halve perception times?

- Significant stabilisation of workload and reporting sites
- What does this mean? How can this be done?

Overview
1. Context and problem
2. Research approach
3. Simulation model structure
4. Management strategies
5. Conclusion
Conclusion

- The oscillations are primarily caused by long time delays related to customer quality perception and changes to the number of reporting sites
- Goal: Stability (sufficient service to sufficiently many)
- Adding more resources does not solve the problem – rather makes it worse
- Reducing perception times for QoS has a dramatic effect on stabilisation.
- Future challenge: How can we implement this insight in practise?

A historical perspective: Building up your Constituency

- In even the oldest presentations on CSIRTs the importance of building up your constituency was highlighted
- Direct impacts were not known – beside funding – before
- Calling for more staff and resources might still be necessary, but not for this reason
- Define the right service level, get resources right and then communicate, communicate, communicate, ...