Carnegie Mellon
Software Engineering Institute – Europe

Effectiveness of Proactive CSIRT Services

Johannes Wiik, Ph.D. Fellow
Prof. José J. Gonzalez
Agder University College
Faculty of Engineering and Science
Grimstad, Norway

Dr. Klaus-Peter Kossakowski
Carnegie Mellon University
Software Engineering Institute
Frankfurt, Germany

Overview

1. Proactive CSIRT Services
2. Organisational Learning
3. Review of the Advisory Service
4. Learning as a Feedback Process
5. Conclusion

CSIRT's Mission

- A CSIRT's mission is:

to be a focal point for preventing, receiving and responding to computer security incidents

from: Killcrece, G., et al. (2003b). State of the Practice of Computer Security Incident Response Teams (CSIRTs). Pittsburgh, PA, USA, CMU/SEI.

Proactive Services are Key

- CSIRTs need to deliver more proactive services to stay effective
- CSIRTs have historically – from the beginning – provided such services
  - the advisory service is proactive in scope and is being provided since 1989
- there are hardly any studies related
  - to what extent existing proactive services are indeed effective
  - or how to make them more effective

Our Approach

- CSIRTs facilitate learning between information providers / vendors and it's users
- We view all proactive services as cross-organisational learning processes
- We evaluate and compare two proactive services:
  - The common advisory service as an example of an existing service, and
  - Neighbourhood watch (NBHW) as a new service that builds on the advisory service.



What does NBHW mean?

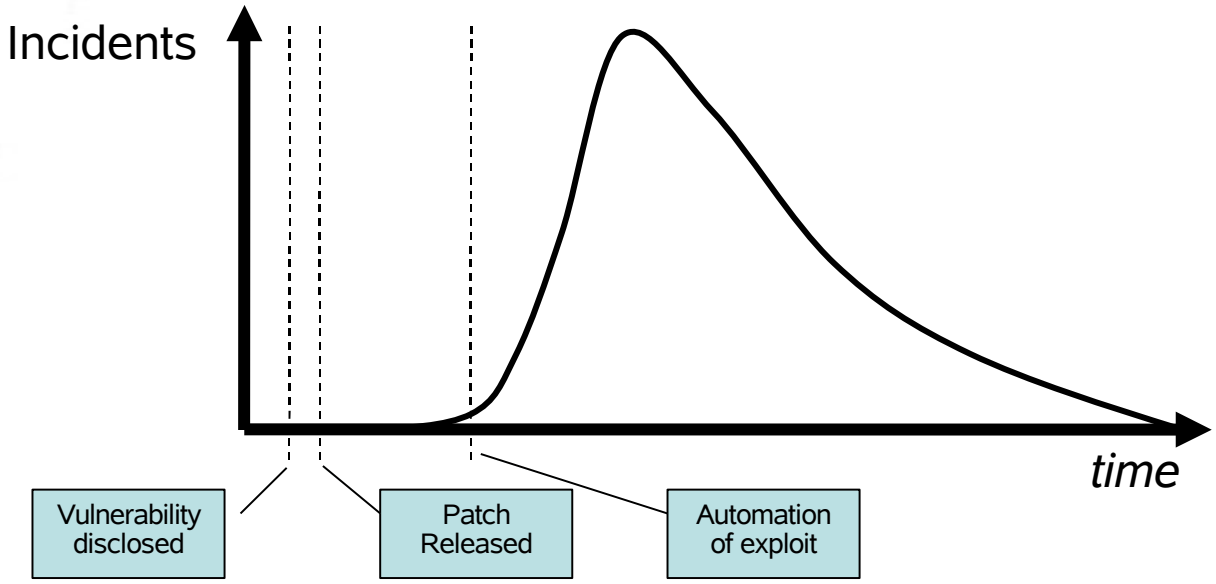
- Scan constituents for any detectable security vulnerability (from the outside)
  - on reachable systems
  - within defined boundaries
  - as agreed before
- Provide comprehensive reporting to the constituents about the findings
  - changes in networks (i. e. new systems)
  - changes on systems (i.e. new ports)
  - changes in security posture (i.e. new vulnerability or advisory)

Research Questions

- What are the weaknesses of the traditional advisory service?
- Can NBHW overcome some of these weaknesses?

Please note: We do not expect that the traditional advisory service becomes superfluous!

Vulnerability Life Cycle



We would rather not argue on a specific time period here, but as new vulnerabilities are continuously disclosed, a hardened system will inevitably oscillate between a vulnerable state when a vulnerability is disclosed, and a hardened state when a fix or a work around has been applied.

Room for improvements?

- The goal of any proactive service must be
  - to provide the information about existing vulnerabilities and available solutions
  - before automation of an exploit is taking place
  - to allow mitigation efforts from all parties involved

What needs to be done?

- For this to happen, a CSIRT has to help its constituency to learn.
  - Indeed this is the purpose of the advisory service.
  - Nevertheless there seems to be several barriers that need to be overcome for effective learning to take place.

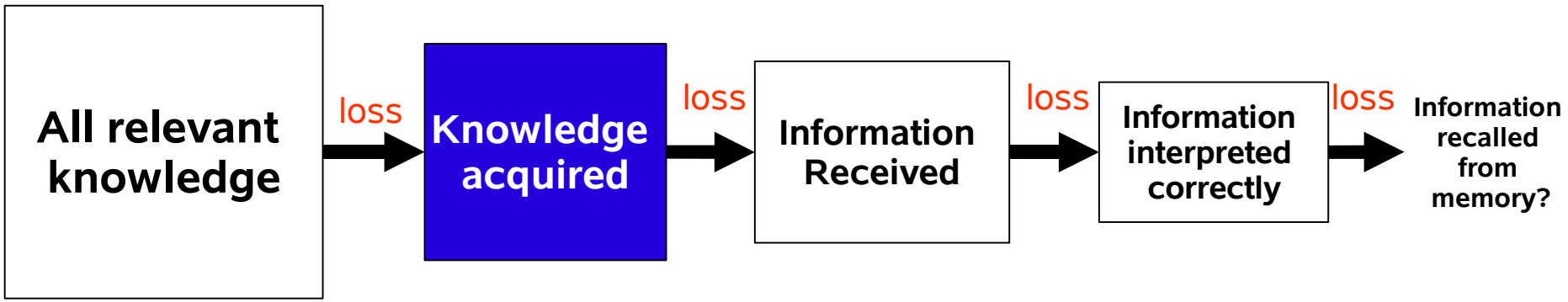
To be proactive, we must learn in advance!

A good way to start understanding cross organisational learning is to use Huber's framework of 4 important contributing processes for organisations to learn

- Knowledge acquisition
- Information distribution
- Information interpretation
- Organisational memory

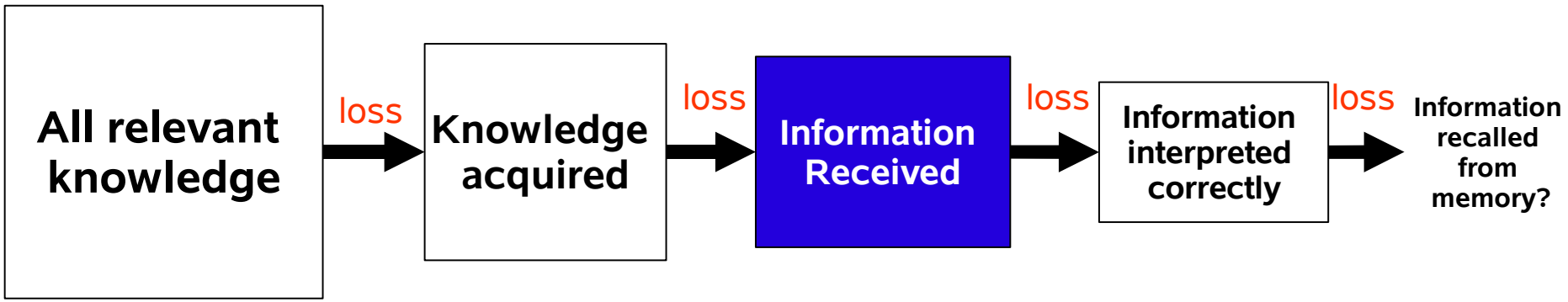
Advisory service – Knowledge acquisition

- How do we know it is the right information for the constituency?
  - Lack of relevant information makes it less useful
  - Irrelevant information is annoying and creates overload



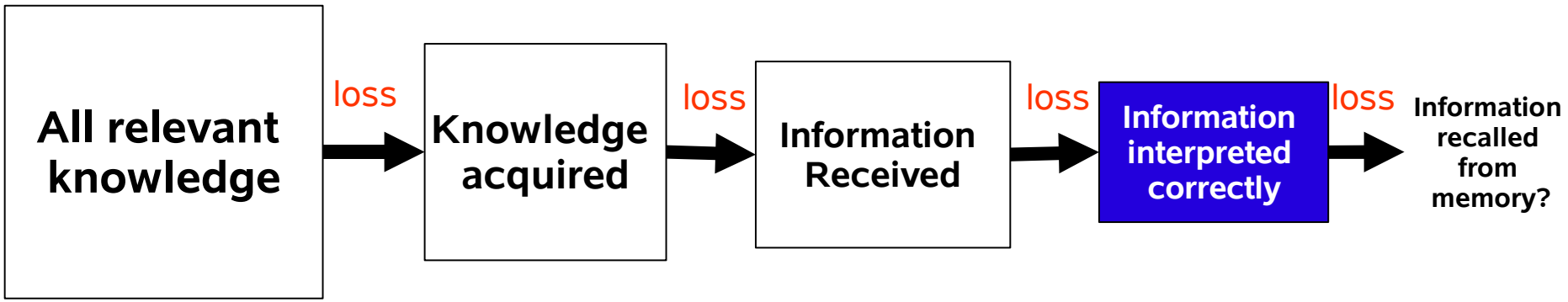
Advisory service – Distribution

- How do we know that the information is received?
  - If we do not reach the right people it is less useful
  - Untimely information does not allow them to get the job done in time



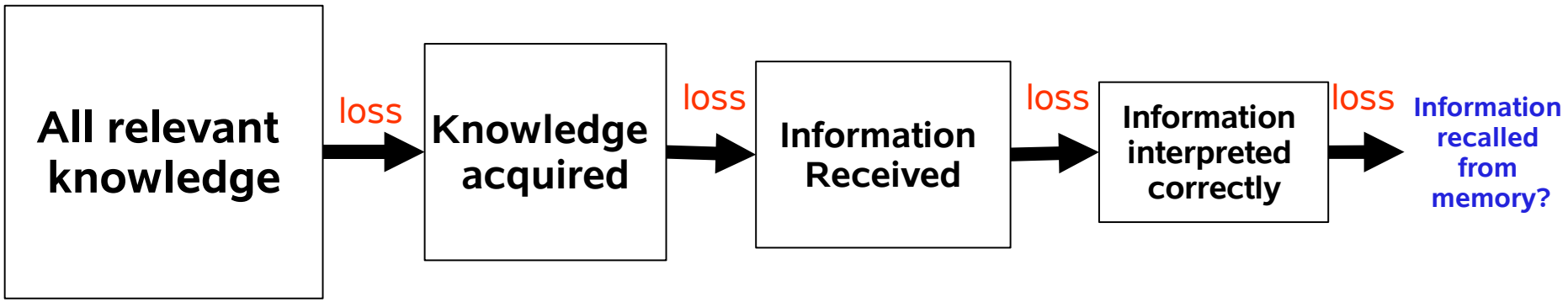
Advisory service – Interpretation

- How do we know that the information is interpreted correctly?
  - If they don't realize the relevance they do not act upon it
  - If they do not understand they cannot act upon it

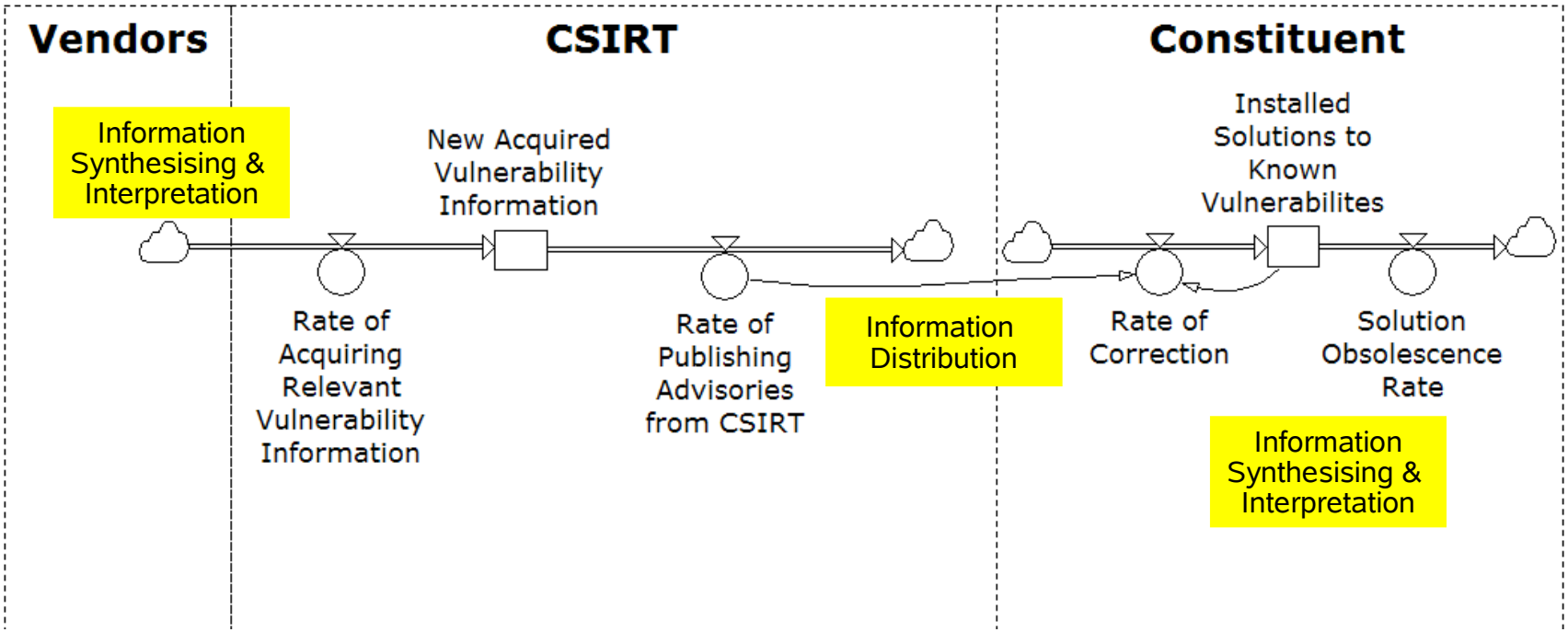


Advisory service – Organisational Memory

- How do we know that the information is kept available?
  - If it is not available it might not be used to re-install machines



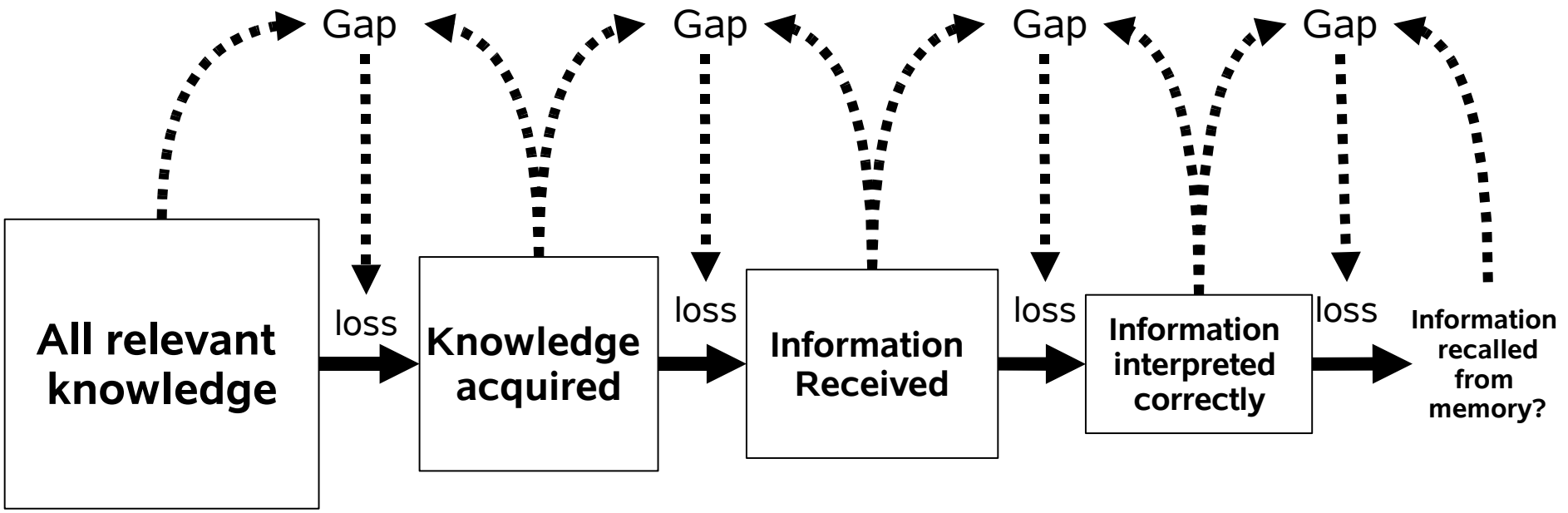
Advisory Service



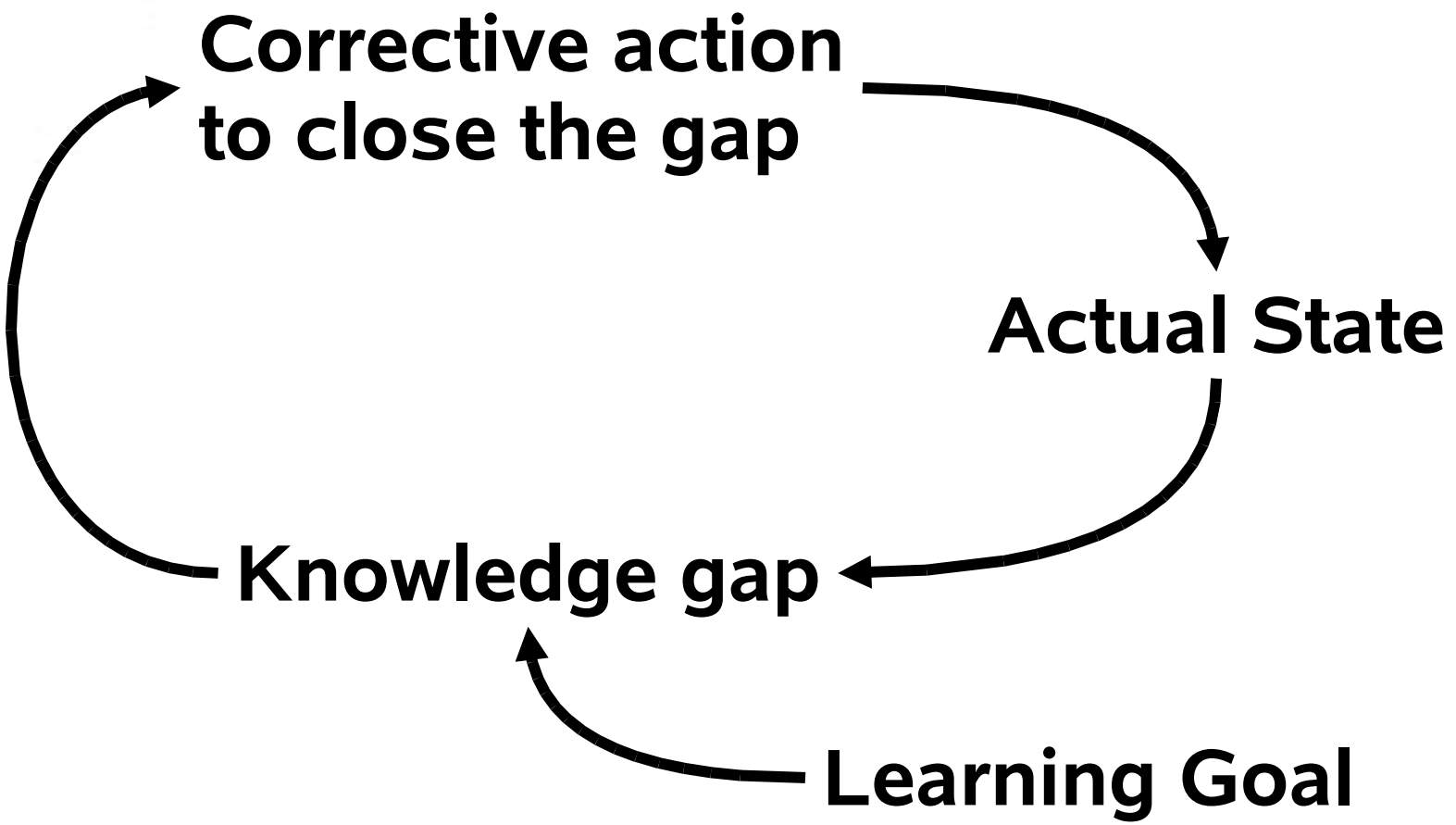
In practise, the advisory service does not provide organisational memory!

If we know the gaps, we can reduce the loss

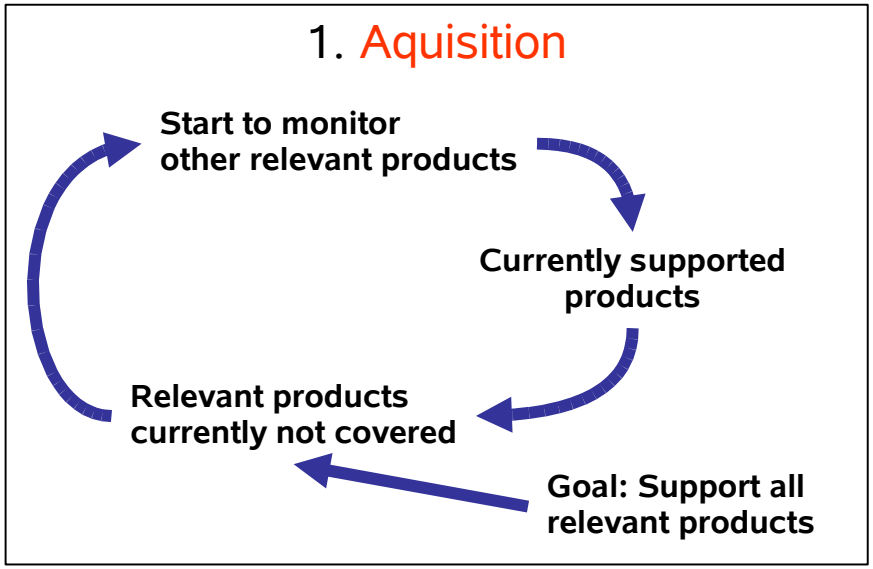
Neigbourhood watch can facilitate all these processes on a continuous basis

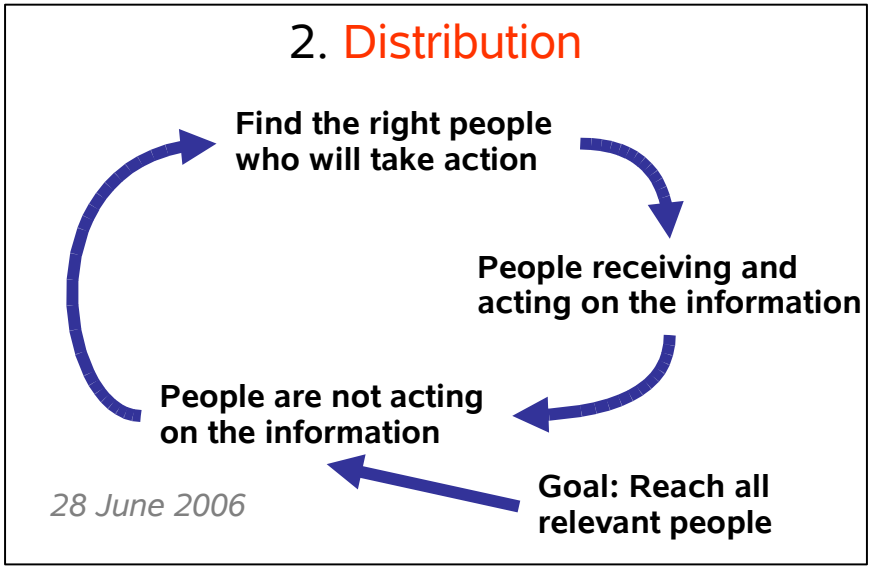


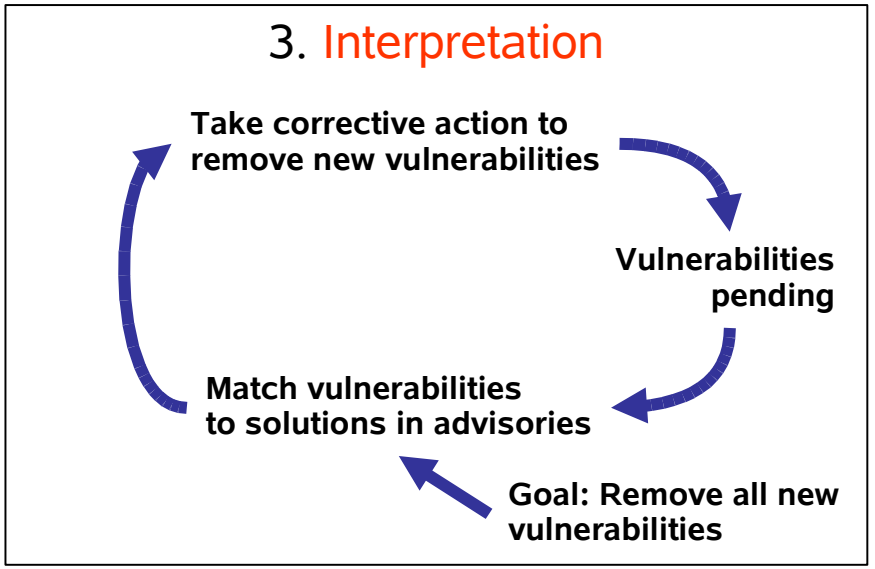
Learning is a Feedback Process



Learning means “Closing the Gaps“







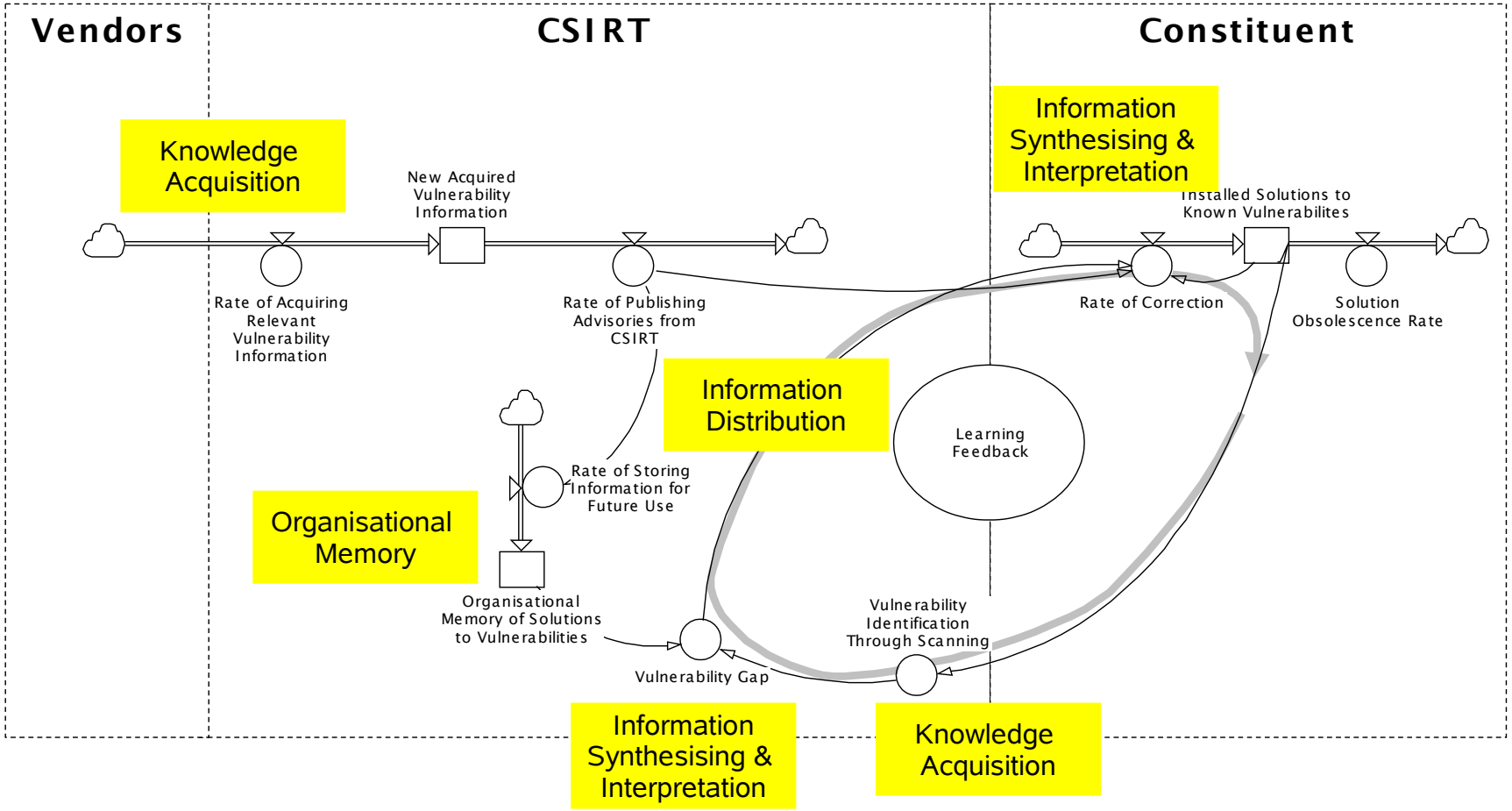
What is different about NBHW?

- The CSIRT can now acquire knowledge about actual vulnerabilities
  - The gap between the actual and the desired state can be identified
  - Reintroduced vulnerabilities will be identified accordingly
- New advisory information can trigger improved actions
  - ad hoc scans to inform administrators
  - assess threat level based on the past

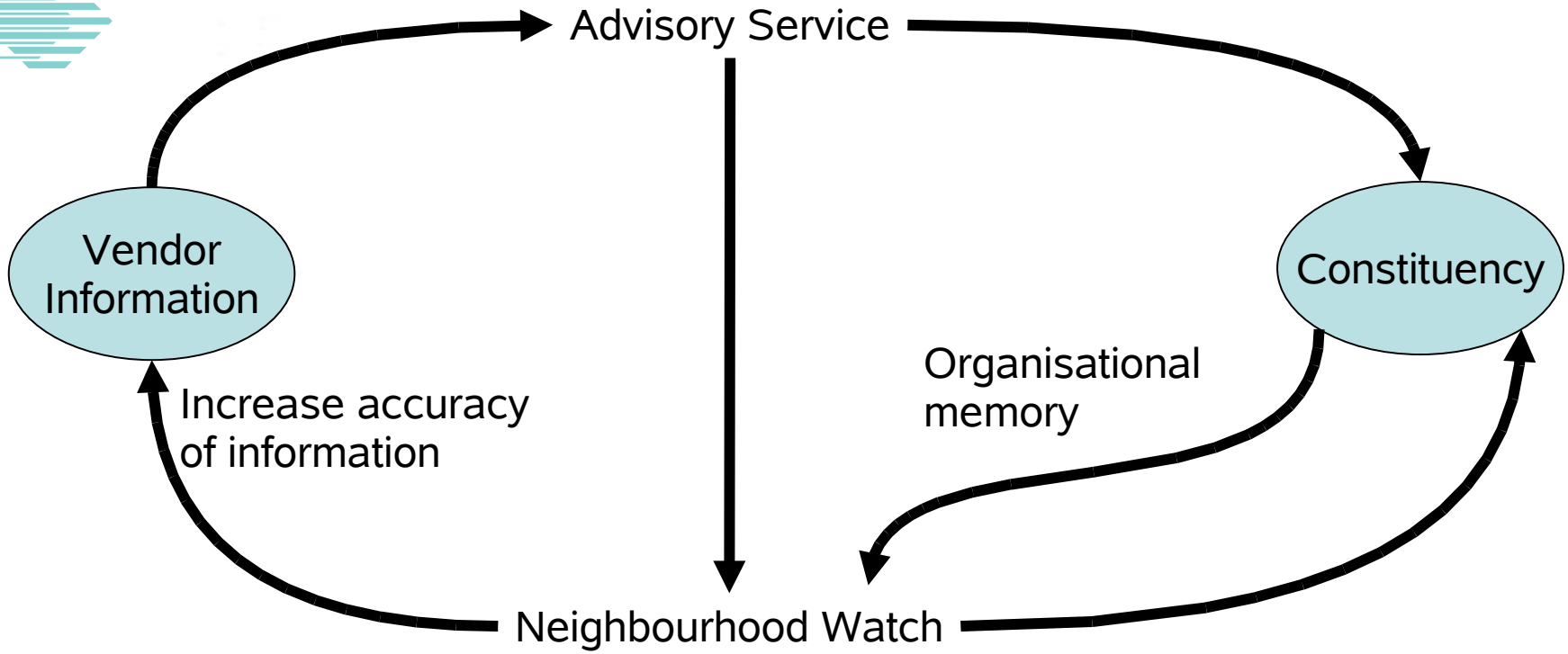
Creating a Feedback loop

- Continuously learning need to take place.
  - The goal is defined by the organi-sational memory of available solutions
- Without the organisational memory no feedback loop can be created
- Organisational memory is instrumental
  - to avoid the “out of sight out of mind” mentality
  - to take action before it is actually too late

Neighbourhood Watch
– Learning across organisational boundaries



Learning feedbacks



- Organisational memory, reuse of information
- Synthesising information

„Unlearning“

- NBHW will enable organizations to institutionalize more proactive measures
- But there will be long time delays, even when compelling evidence is available.
  - A lot of **“unlearning”** has to take place, as people have to disregard what they considered to be the “truth” before
- Changing a mental model is challenging!

Conclusions

- Indeed the potential of proactive services should be seen in a cross-organisational learning process context.
- Only if the constituents are enabled to learn from the experiences of the past and from others effectively, this potential will come true.

Conclusions (2)

- All CSIRT related activities are impacting each other and should not be seen as separate activities.
- Current management approaches do not consider this aspect.
- CSIRTs need to revisit their services and interdependencies not yet addressed in their current setup.