CERT.be
The Federal Cyber Emergency Team

Leaving our island:
a communication and business strategy for a National CSIRT

Christian Van Heurck
Coordinator

24th annual FIRST conference – Malta - 17-22 June 2012

Agenda

- Core idea
- Case Introduction
- Techniques & Results
- Case results
- Lessons learned
- Q&A

Core idea

EXPERTISE

is essential

for any

CSIRT service

Core idea

COMMUNICATION

is an

essential service

of any

CSIRT

Case introduction

CERT.be

The federal cyber emergency team

a service of **Fedict**
operated by **Belnet**

CERT.be history

- **Belnet CERT** in 2004
- Grew to **3 FTE** (+ Belnet)
- **CERT.be** created in 09 / 2009
- Grown to **8 FTE** (+ **Belnet**)

CERT.be initial assets

- **Part of CSIRT community**
- Contacts with National partners (LE, CERT MIL)
- **Neutrality & Confidentiality**
- **Trusted** by those who knew us
- **Key role in Belgian Internet landscape**
- **Experience in incident handling**
- **Specialists**
- **Motivated team**

CERT.be initial weaknesses

- **Not known by all those needed**
- **NREN CSIRT model did not scale**
- Too much focus on technical expertise
- No real communication strategy
- **Expectations & Ambition**
- **Team & budget size**
- **No solid contract nor mandate**
- Political situation

Techniques and results

- CFT to help with **communication plan**
- Start in 09/2011 with **expert** in:
  - start & growth strategy for business
  - marketing ROI
  - corporate positioning
  - product & service positioning
  - …
- He knew **nothing** about a CSIRT
- He **loved** this case!

Some interesting results

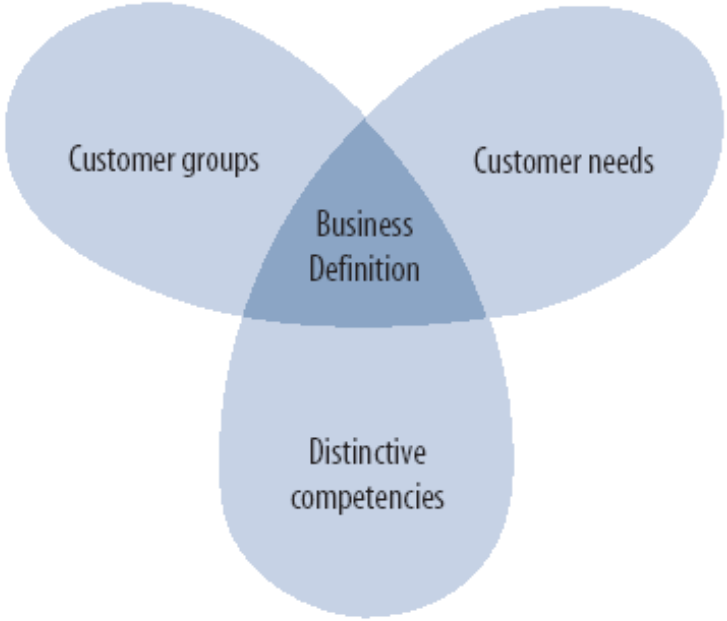
- **CERT.be communication situated on different levels**
- 3 **external** levels
  - Brand or corporate = mission, vision
  - Market = segmented with different goals
  - Service = positioning & describing services
- 2 **internal** levels
  - Amongst CSIRT community
  - Within Belnet and Fedict
- **Communication is an essential CERT.be service**

Some interesting results

- **CERT.be business definition model**

Which customers are being served?

What needs are being fulfilled?

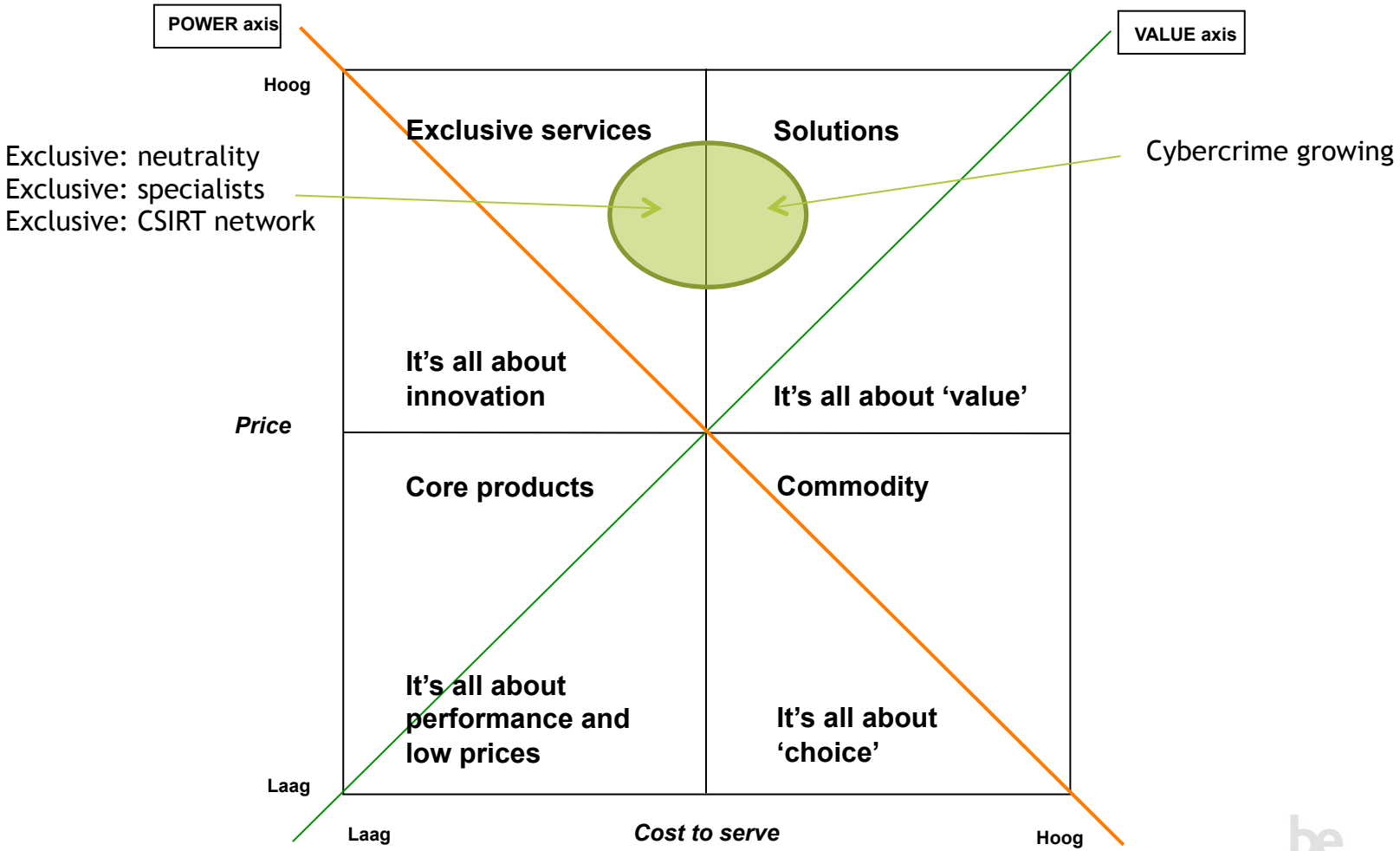


How do we fulfill these needs?

Some interesting results

- **Value disciplines model** (Treacy and Wiersema)
  - Operational excellence
    - efficiency, monitoring & measuring, static portfolio
  - Product leadership
    - R&D, flexible, innovative
  - Customer intimacy
    - large portfolio, structure close to customer, long term
- **Excel in one – threshold for other 2**
  - Product leaders
  - Price leaders
  - Customer leaders

Some interesting results

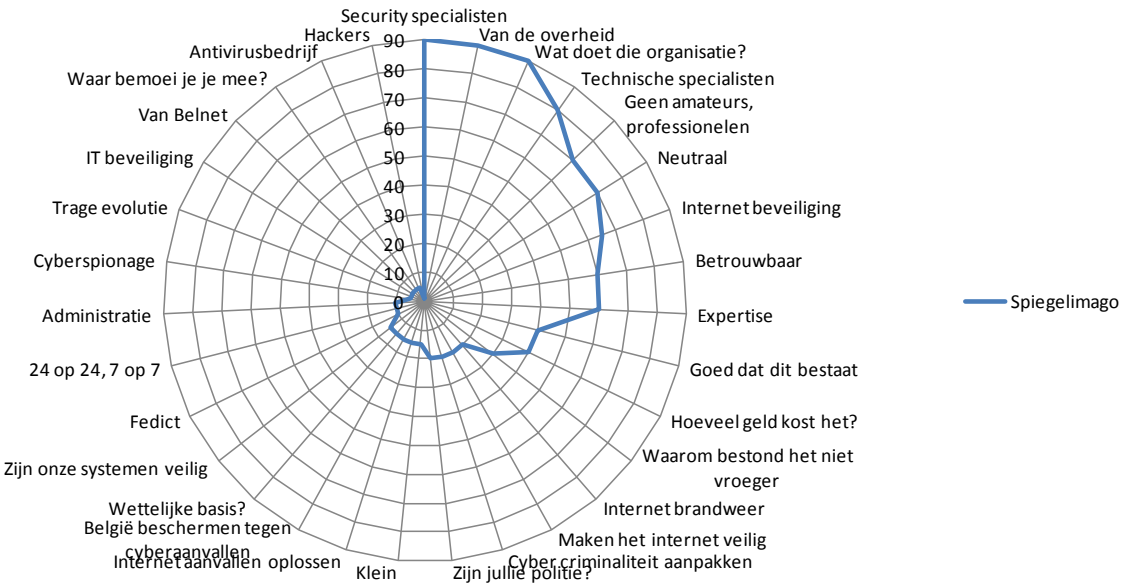


Some interesting results

- **Brand equity profiles for different segments**
  - Actual
  - Wanted
- **SWOT & confrontation matrix**
- **Corporate ideology, mission and vision**
- **KPIs for the service brand CERT.be**
  - Reliability
  - Responsiveness
  - Tangibles

The list goes on …

- **Brand positioning**
- **Image model**
  - Image - Mirror image – Wanted – Ideal - Image matrix



And on …

- **Value proposition**
- **Product positioning matrix**
- **12-cell matrix: define essential criteria**
  - Take action
  - Use opportunity
  - Pay less attention
  - Marginalize attention
- **Positioning**
- **Brand structures**
- **Endorsed brand structure for CERT.be**
- **Communication planning**
  - Tactical planning

Results produced

- **Communication plan for CERT.be**
  - Finished in 10/2012
    - 20 page report
    - 69 page presentation
    - Spreadsheets with planning
  - Presentation to stakeholders
  - Spreadsheet with planning
  - Business positioning
  - Positioning tagline
  - Business definition model
  - Corporate ideology
  - Brand strategy

Results produced

- **Communication strategy for CERT.be**
  - Strategic goals
  - Communication goals
  - Target groups
  - Communication goals by target group
  - Operational communication
    - Planning
    - Means
    - Evaluation parameters

Case results: opportunity

- **DNS-changer malware**
  - Applied what we learned
  - Positive results!

Case results: CERT.be initial weaknesses

- **Not known by all those needed**
- **NREN CSIRT model did not scale**
- Too much focus on technical expertise
- No real communication strategy
- **Expectations & Ambition**
- **Team & budget size**
- **No solid contract nor mandate**
- Political situation

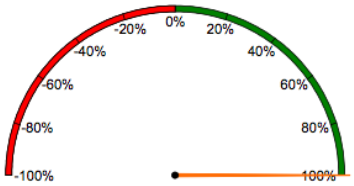
Case results: media barometer

Barometer + van february 2012

BELNET

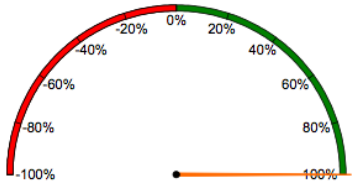
CERT.BE (26364)

Evolutie vergeleken met vorige maand



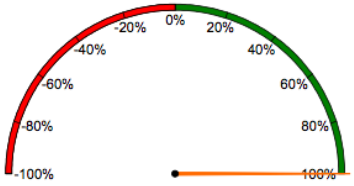
14446,77%

Minimum aantal personen die door de info werden bereikt



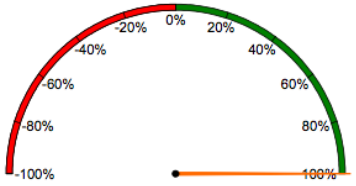
N/A

Aantal dagbladartikels



N/A

Aantal nederlandstalige artikels



900,00%

Aantal franstalige artikels

Lessons learned

- **IT WORKS!**
  - Engaging communication profile
  - Impact on workload
  - Impact on project planning
  - Change “state of mind”
  - No silver bullet
  - Journalists are important
    - Media training
    - Symbiosis
  - Have to follow the news
  - More efficient in the end

Conclusion

COMMUNICATION

is an

essential service

of any

CSIRT

christian.vanheurck@cert.be