VINNOVA
Sweden's Innovation Agency

LUND UNIVERSITY

debricked

Structured communication of vulnerabilities in open source software: tailoring information to different recipients

Master thesis project in the Vinnova project HATCH at the Department of Computer Science and Debricked

EMMY DAHL & MICHAELA KARLSSON

Background

- **Exploitation** amongst most common reasons to security incidents (NCSC 2020)
- Global average cost of a data breach is **$3.9M** (IBM Security Report 2019)
- Number of vulnerabilities published each month (NVD Database)
  1999: **75**
  2018: **1380**
- Globally lacking **2.93M** cyber security experts (CNBC 2019)

Previous research

A survey-based study conducted in 2019[1] concluded the following:

- In general it exists an industry openness towards communicating vulnerabilities
- Communication of vulnerabilities is mainly done reactively
- The total cybersecurity of a product often depends on collaboration between several actors in a value chain
- Future studies within the area are needed in order do derive guidelines for how such communication should be structured

[1] M.Borg, U.Franke, M.Hell, M.Höst, and T.Olsson. *Sharing of vulnerability information among companies – a survey of Swedish companies.* 2019.

What do we need to know?

RQ1 What type of recipients of vulnerability information is there in a company?

RQ2 What kind of vulnerability information does each type of recipient need within the frame of their profession?

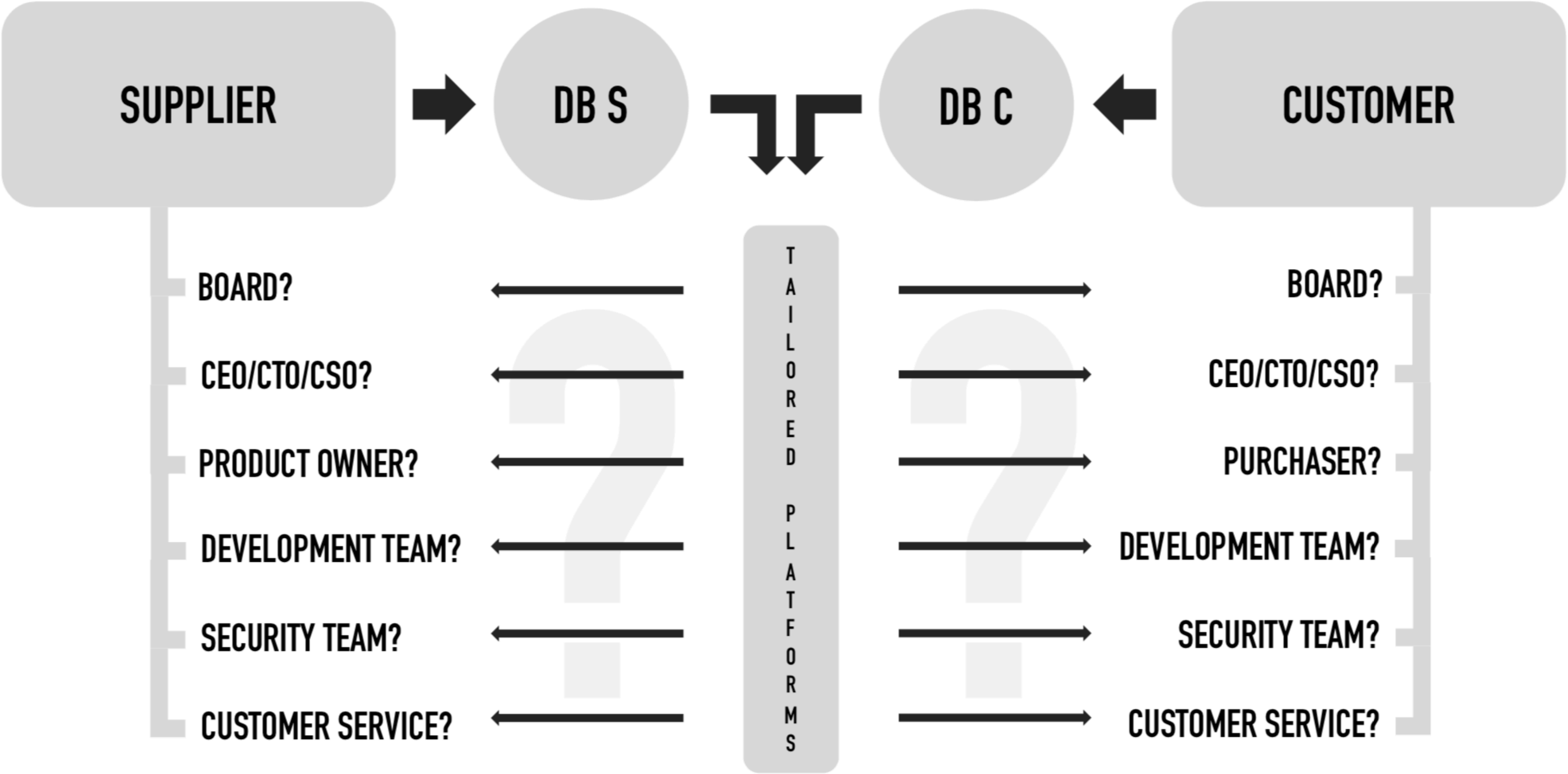
RQ3 How should vulnerability information be tailored and presented on a web platform for each type of recipient?

The objective is a generic solution applicable regardless of market.

Many company roles

DB S = SUPPLIER DATABASE

DB C = CUSTOMER DATABASE



Methodology

- **Interviews!** With people who come across vulnerabilities in their jobs, working at different companies, in different sectors and having different roles.

- **Literature Study!** Collecting already existing research and theory to use when analyzing our collected data.

- Want to contribute? Reach out to us during the break!

What are our findings so far?

- **Some roles to tailor information to are:**
  Product owner, developer, triage responsible, key account manager, CTO, Board

- **How should the information be presented?**
  Dashboard with different views!

- Example of views:

DEVELOPER

TRIAGE

CUSTOMER CARE

BOARD

What are our findings so far?

- **Communication can look very different in different companies**
  Lack of documentation and aligning of information.

- **Common ground for communication**
  General severity scoring as a first screening

Questions?

Don’t forget to sign up for an interview!

AM I READY FOR THIS INTERVIEW?
FALSE. THE QUESTION IS, IS THIS INTERVIEW READY FOR ME?