Responsibly fixing cross-border vulnerabilities

The practical approach to understanding and working with vendors all over the globe

Kirils Solovjovs *31.05.2016* *Tallinn*

PSA

Public Scaremongering Announcement

- Where was your laptop last two days?
- The evil maid knows.
- Never forget!

YOU HAVE NO ONE
TO BLAME BUT YOURSELF
AND EVERYONE
HAS YOU TO BLAME, TOO

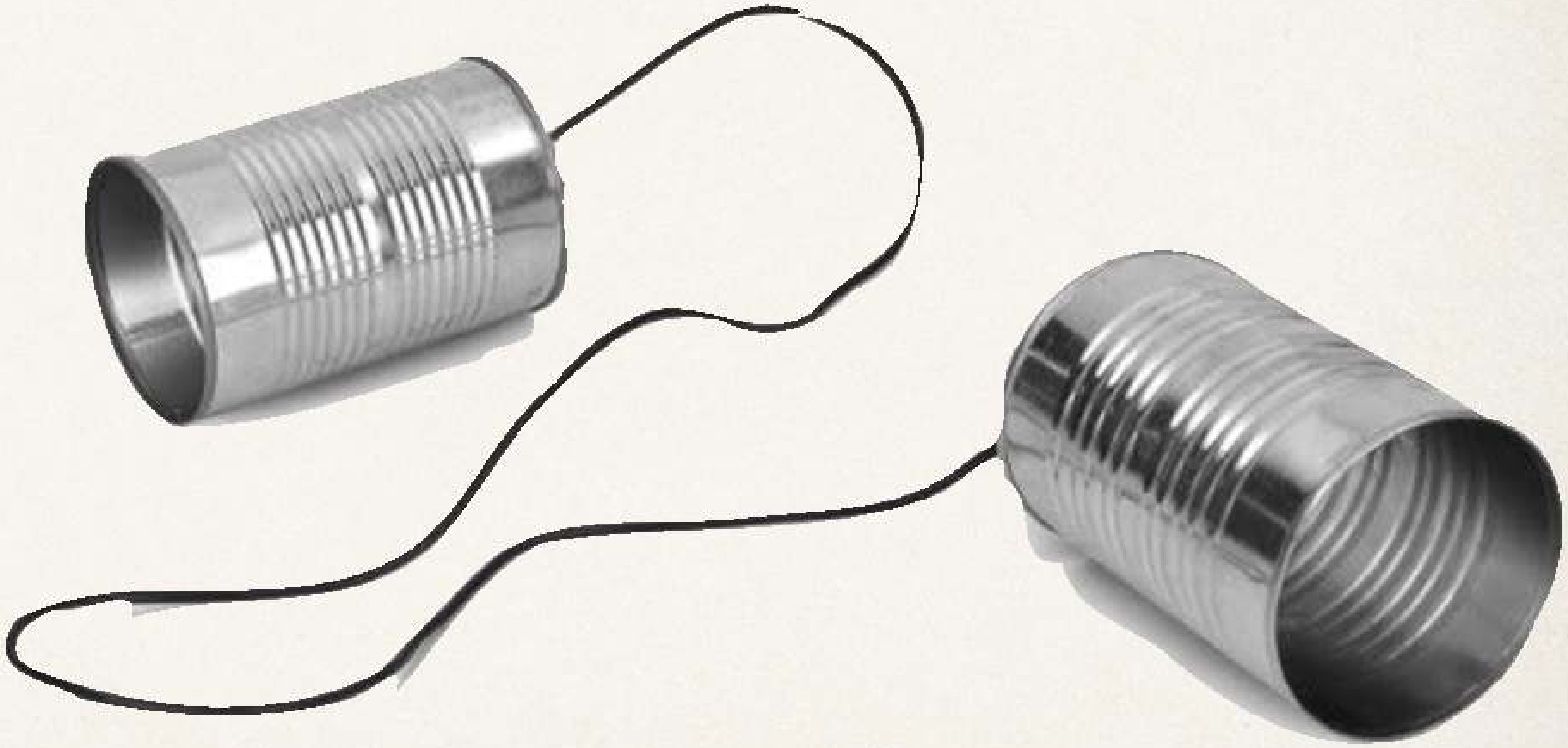
There is no market demand for a security component in your service or product

DEMAND =	SUPPLY
Low	Low

So what (are the implications)?

Tech implications

- No patches, no patching
  - Patches, but still no patching
- Less % of healthy nodes
  - Botnets thrive, more spam
- Larger breeding grounds for the next security incident



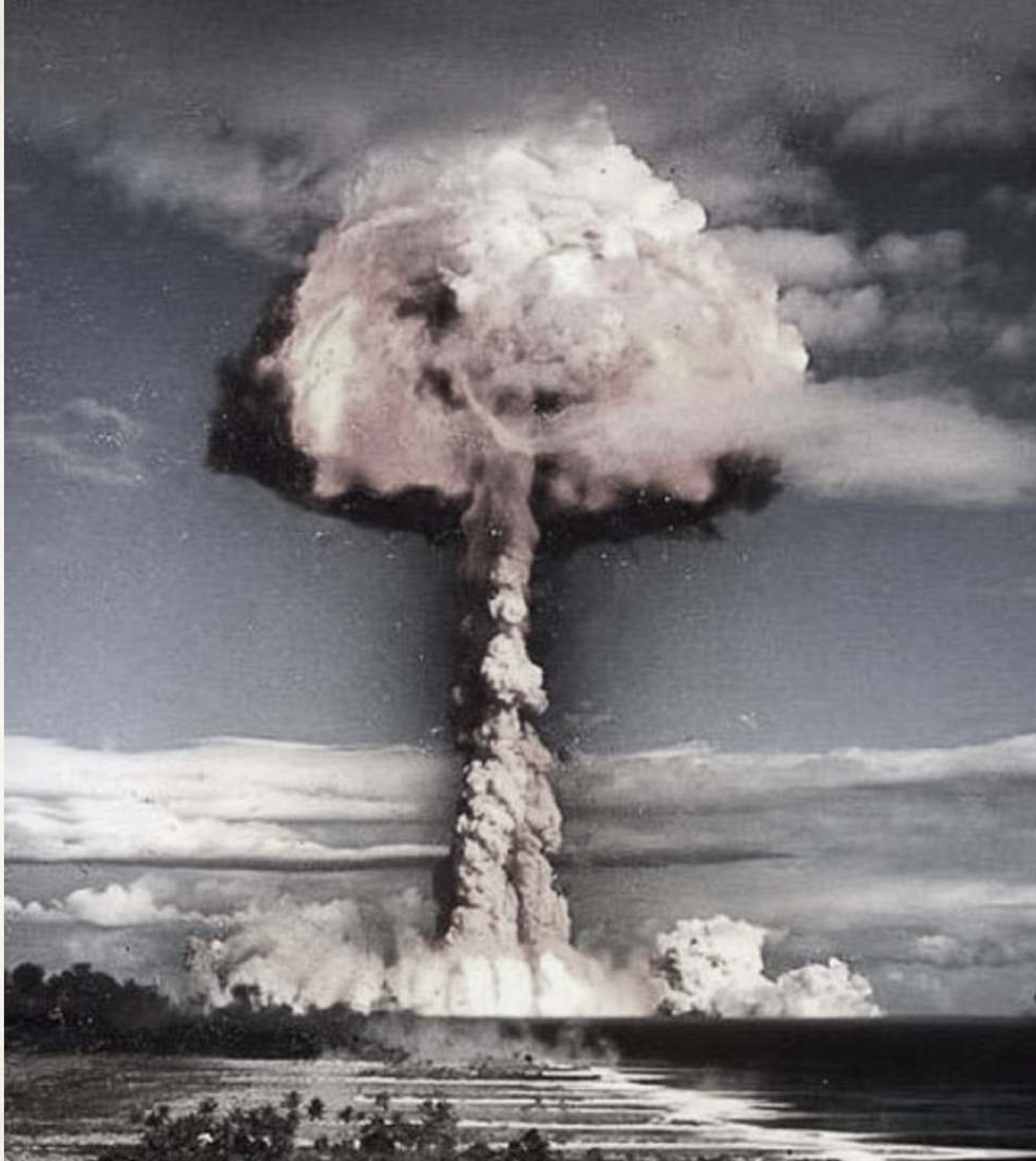
Privacy implications

- Cyber-peeper in your bedroom
- Authentication becomes meaningless
- Customers continue to lose their data

HELLO? I WOULD LIKE TO REPORT AN OUTRAGEOUS PRIVACY BREACH.
I FOUND THIS BOOK ON MY DOORSTEP WHERE MY NAME, FULL ADDRESS AND PHONE NUMBER ARE ALL DISPLAYED IN CLEAR TEXT!!
PHONE BOOK
MANU CORNET

Legal implications

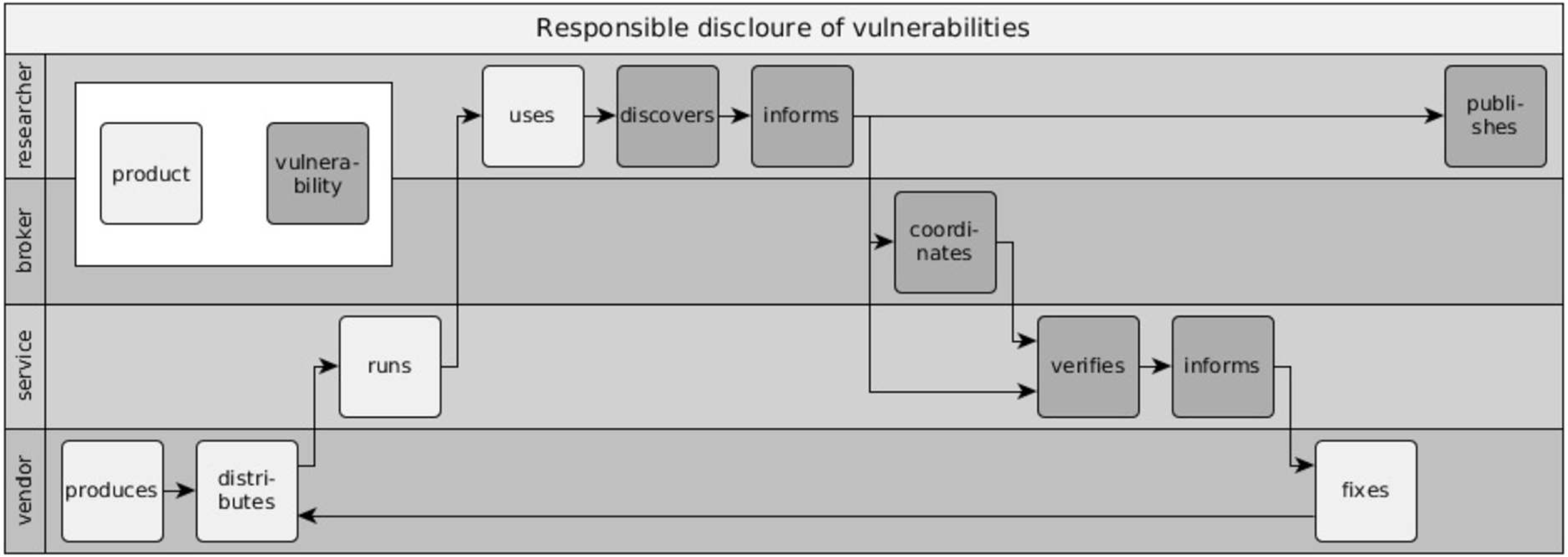
- Consumers, government, employees and partners suing the service provider
  - Target, 2013
- Company or government suing the researcher
  - Florida's Office of Elections, 2016
- Government suing the vendor
  - Asus, 2014
- ~~Company suing the vendor~~



Responsible Disclosure Process to the rescue

What is RDP?

- Responsible Disclosure Process:
    - is a type of vulnerability resolution process
    - initiated by a researcher
    - requires good-faith communication effort by all
    - allows vendor to fix the vulnerability in a timely manner
    - ultimately ends with a public disclosure



Responsible discloure of vulnerabilities

Cross-border security is not easy

- Traditions and culture
- Limited face-to-face possibilities
- Variable geographical impact
- Legislation
- Time zones

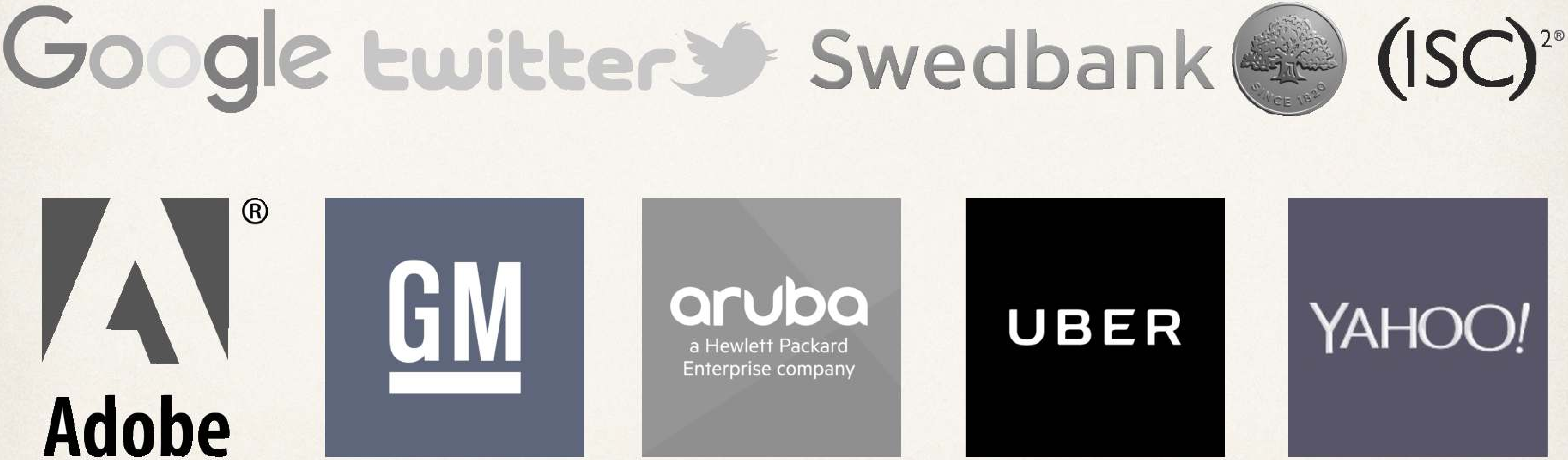
“I have forwarded your information to the appropriate party. If there is an interest, someone will contact you.”

– First and last time I ever heard from [redacted]

"We truly appreciate the information that you have brought forward to us. But for obvious security reasons, it is [redacted] policy to never discuss engineering matters outside of [redacted] and thus we will not be commenting further on this issue."

– [redacted] manager after "the info has been dealt with"

Many companies choose to be part of it



Some choose not to

But are often left with little choice

The middleman

Responsible Disclosure brokers (white)

- Entities acting as a middleman between the researcher and the vendor
  - Private brokers
    - Hacker one
    - Bug crowd
  - Public brokers
    - CERT/CC and other CSIRTs
    - Media

Other brokers (grey)

- Entities acting as a middleman between the researcher and **other parties**
  - Agnostic brokers
    - Full-disclosure mailing list
  - Commercial brokers
    - Zerodium
    - ReVuln
    - Exodus Intelligence

Illegal brokers (black)

What can a state do to enable RDP?

Netherlands

> “Whenever a hacker gets in touch directly and safely with the owner of the IT-system regarding a discovered vulnerability and no data is manipulated or removed then there may be a case of RD. This means there is no reason for a criminal investigation and for a criminal prosecution.”

–NL Public prosecutor guidelines, 2013

Latvia – a step further

> “Arbitrary accessing an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if they are directed against automated data processing systems that process information related to State political, economic, military, social or other security, shall be excluded from criminal liability, if a person has followed the Responsible Disclosure Process.”
>
> *– The Criminal Law (draft amendment), 2016*

Discussion time!

Responsibly fixing cross-border vulnerabilities

Kirils Solovjovs 31.05.2016 Tallinn

@KirilsSolovjovs

kirils@possiblesecurity.com