
Cyber security is a team sport
Who shares wins
Nordic Financial CERT
For members, by members

Cyber & the importance of cooperation

Morten Tandle, Nordic Financial CERT

Personal story – early experience

Why do the cyber attackers win?

- Rapid pace of change
  - Technology
  - Digitization
  - Cybersecurity
    - Red (attack) vs blue (defense)
- Distributed global nature of the internet - borderless
- Barriers to sharing

Ransomware: Publicly Reported Incidents are only the tip of the iceberg

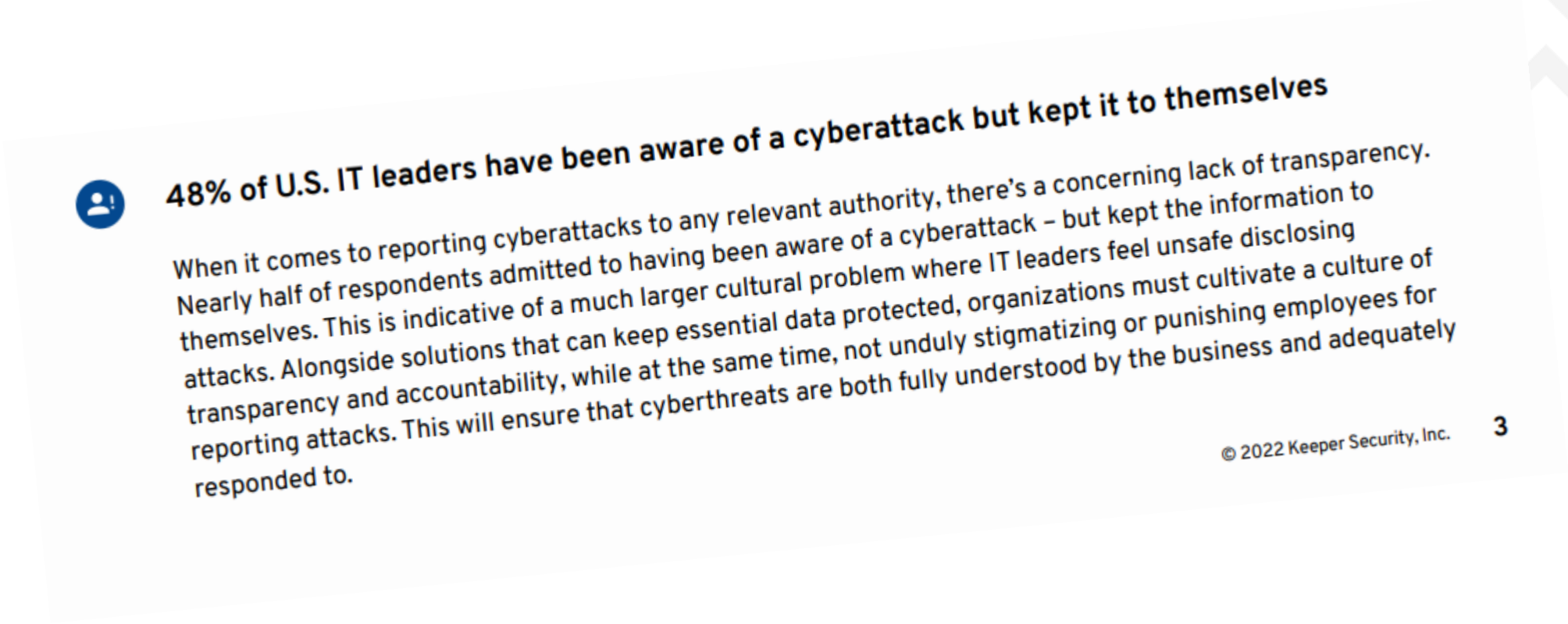
The threat landscape report on ransomware attacks published today by the European Union Agency for Cybersecurity (ENISA) uncovers the shortcomings of the current reporting mechanisms across the EU.

Published on July 29, 2022

Cyber – non-transparent ‘service stacks’

- «Hidden dependencies»
- The digital value chains are long and non-transparent – poorly understood

Example 1 – barriers



48% of U.S. IT leaders have been aware of a cyberattack but kept it to themselves

When it comes to reporting cyberattacks to any relevant authority, there's a concerning lack of transparency. Nearly half of respondents admitted to having been aware of a cyberattack – but kept the information to themselves. This is indicative of a much larger cultural problem where IT leaders feel unsafe disclosing attacks. Alongside solutions that can keep essential data protected, organizations must cultivate a culture of transparency and accountability, while at the same time, not unduly stigmatizing or punishing employees for reporting attacks. This will ensure that cyberthreats are both fully understood by the business and adequately responded to.

https://www.keeper.io/hubfs/Reports/2022-US-Cybersecurity-Census.pdf

Example 2 – why?

- Solarwinds case (2020-21)
  - You are all familiar with it.
- What if those early victims did not share?
- How did sharing and collaboration help?

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

Cyber warfare + Add to myFT

What do we know about the SolarWinds hack?

Security officials race to probe one of the most sophisticated cyber attacks of recent years

Save

Hundreds of thousands of organisations around the world rely on software from SolarWinds to manage their IT networks © Financial Times

Helen Warrell in London and Hannah Murphy in San Francisco DECEMBER 14 2020 92

Example 3 – situation picture/threat understanding

- Bangladesh central bank robbery (2016)
  - You are all familiar with it
- High-profile attack in a niche and traditionally high-security area
- How did sharing and collaboration help?

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI

Cyber Security + Add to myFT

How cyber criminals targeted almost $1bn in Bangladesh Bank heist

Theft sends tremors around the world among banks and large corporations that keep big balances

Save

Victor Mallet in Dhaka and Avantika Chilkoti in Jakarta MARCH 18 2016

17

What to share – and how do we get there (1)

DORA CHAPTER VI/Article 40 –
INFORMATION SHARING ARRANGEMENTS

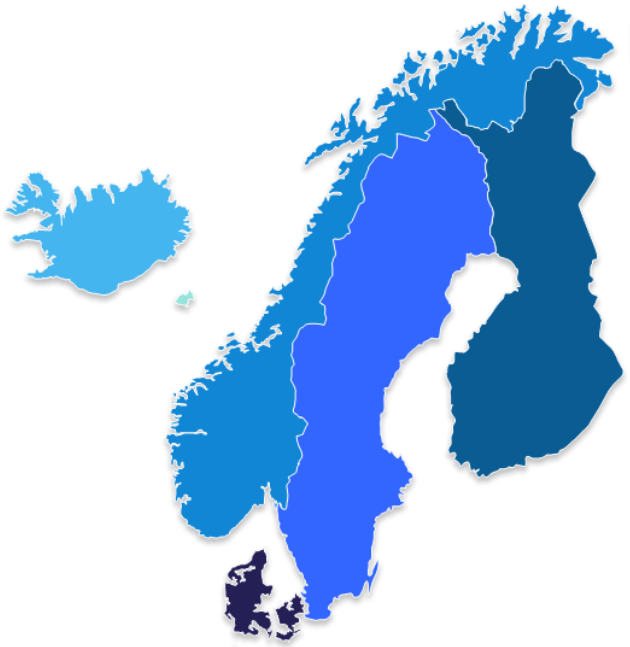
(a) aims at enhancing the digital operational resilience of financial entities, in particular through raising awareness in relation to

- cyber threats,
- limiting or impeding the cyber threats' ability to spread,
- supporting defensive capabilities,
- threat detection techniques,
- mitigation strategies or
- response and recovery stages;

(b) takes places within trusted communities of financial entities;

What to share – and how do we get there (2)

- Create and support sharing communities in circles of interest
- They often work better if
  - Trust is high
  - Participants see the value
  - They are resourced and facilitated



About Nordic Financial CERT (NFCERT)

A non-profit with ~230 members across the 5 nordic countries.

- Creating a vibrant sharing community around cyber defense

MISSION:

Enable Nordic financial institutions to jointly detect and respond to cyber threats and incidents.

A trusted community for sharing and learning

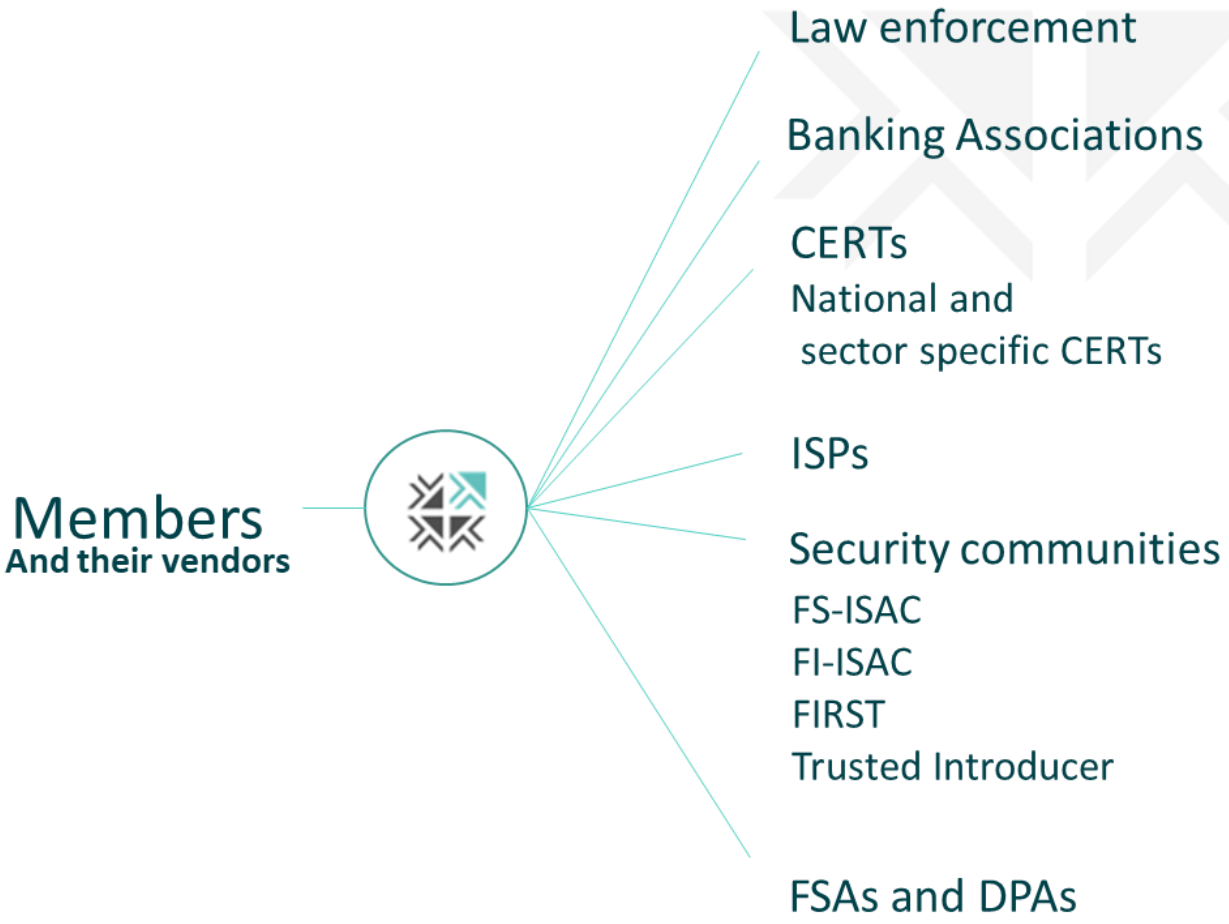
– Our members

Trusted community

– Several communities within NFCERT

Public/private sharing hub

a sharing hub between our members and government/other communities



Trusted community

– NFCERT members get plugged into the external network

Authorities

NSM

CERT.IS

TRAFICOM National Cyber Security Centre

FE CENTER FOR CYBERSIKKERHED

FINANSTILSYNET

FINANSTILSYNET

POLITIET KRIPOS

POLITI

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

Member vendors

tieto EVRY

JN DATA

nets

SDC

bec FINANCIAL TECHNOLOGIES

bankdata

BITS

e-nettet

RB

orange Business Services

SWIFT

Other

norskhelsenett

ENERGI CERT

SUNDHEDSDATA-STYRELSEN

Kraft CERT

NORMA CYBER

Telecom and ISPs

Security communities

FS-ISAC

TI

EU FI-ISAC

FIRST Improving Security Together

Wrapping up

- We need to share and cooperate to successfully defend our digital infrastructure and services

- Sharing and cooperation works best when encouraged and nurtured

- We all use the same technology, and depend on the same infrastructure

→ Sharing communities should be both local and globally connected

Thank you for your attention!

Morten Tandle

E-mail: morten.tandle@nfcert.org

Mobile: + 47 950 25 035

Collaboration and sharing on operative cyber defense

- Outside our membership – EU/Global

  - Most important – FS-ISAC
    An association with >7000 members all over the world. Great sharing community.
  - EU FI-ISAC (supported by ENISA)
    Good EU-level sharing community
  - EMEA Financial CERTS (IL, IT, CH, Nordics)
    Regular sharing
  - FIRST.org – great global IR professional community
  - Trusted Introducer – IR professional community, with good activity in Europe


Nordic Financial CERT