THE PARADIGM SHIFT IN PATCHING REGULATION

UPCOMING EU RULES FOR CYBERSECURITY PATCHING

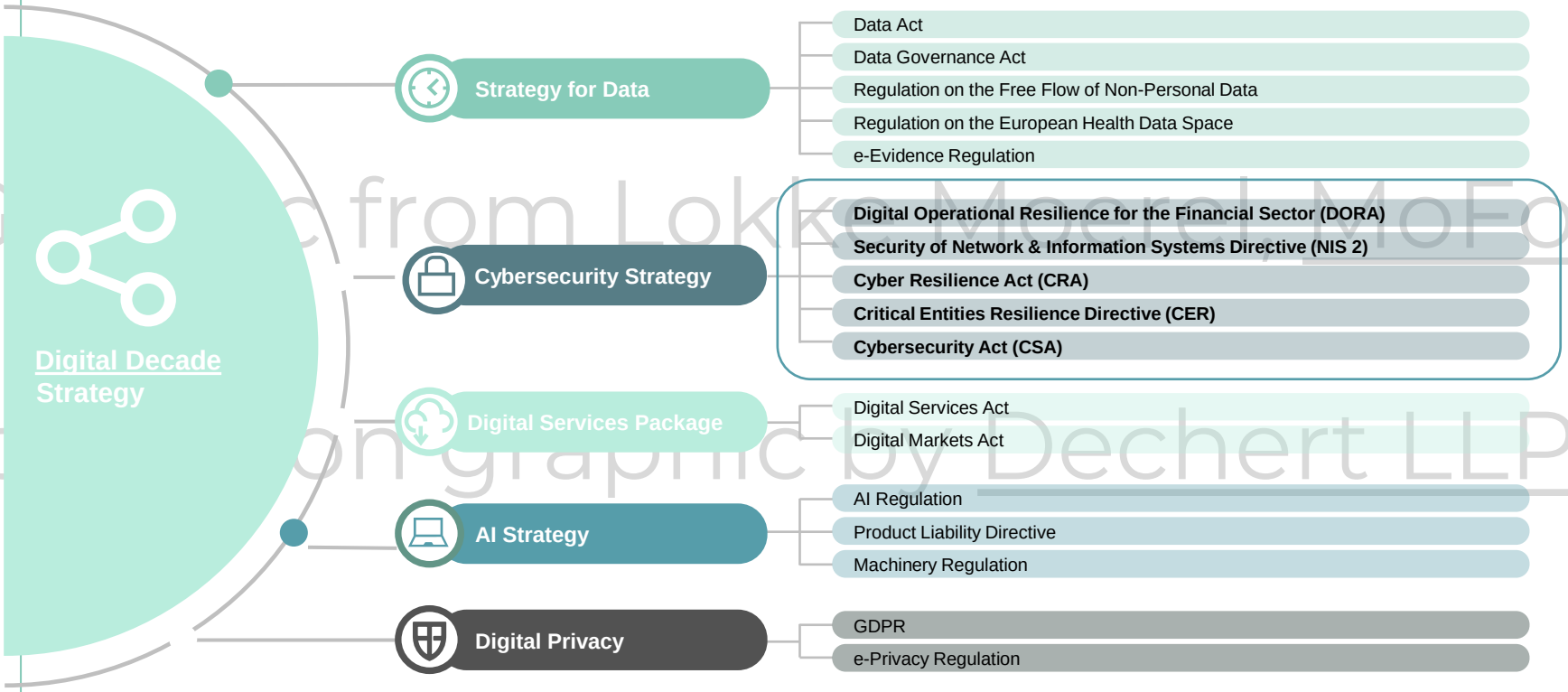
Lisa Rooij

Cyber PhD day 30 April 2024

“PATCHING”

Software and operating system **updates that address security vulnerabilities** within a program or product, and can add new security functions.

EU: Digital Decade Overview



...So let's condense.

Generic Security Requirements

"shall take appropriate technical and organisational measures to protect personal data/safeguard security of their services."

1995 Data Protection Directive & 2002 ePrivacy Directive

Generic Security Requirements
based on risk assessment & standards

"**Taking into account the state of the art**..., shall take appropriate technical and organisational measures to ensure a level of security **appropriate to the risk.**

- including the ability to ensure confidentiality, integrity, availability and resilience

2016 GDPR

Liability for patching violations – data protection

The Law Society Gazette
https://www.lawgazette.co.uk › news › 5111806.article

Firm fined almost £100000 over ransomware attack | News

10 Mar 2022 — Criminal defence firm **Tuckers** Solicitors has been fined £98,000 after failing to

DSG Retail Limited Fined £500K by ICO Following Malware Attack

Posted on January 10, 2020

Notice of reprimand against Telenor Norge AS

NKOM has adopted a fee of 1.5 million

We are notifying of a decision to reprimand Telenor Norge AS for lack of personal data security in the voice mailbox function, and for failure to notify the Norwegian Data Protection Authority.

Equifax fined by ICO over data breach that hit Britons

Credit rating agency Equifax is to be fined £500,000 by the Information Commissioner's Office (ICO) after it failed to protect the personal data of 15 million Britons.

Liability for patching violations – data protection

| News

98,000 after failing to

"Equifax Ltd has received the highest fine possible under the 1998 legislation because of the number of victims, the type of data at risk and because it has **no excuse** for failing to adhere to its own policies and controls as well as the law."

-Former UK Information Commissioner Elizabeth Denham

Norge AS for lack of personal data security in the voice mailbox function, and for failure to notify the Norwegian Data Protection Authority.

K by ICO Following

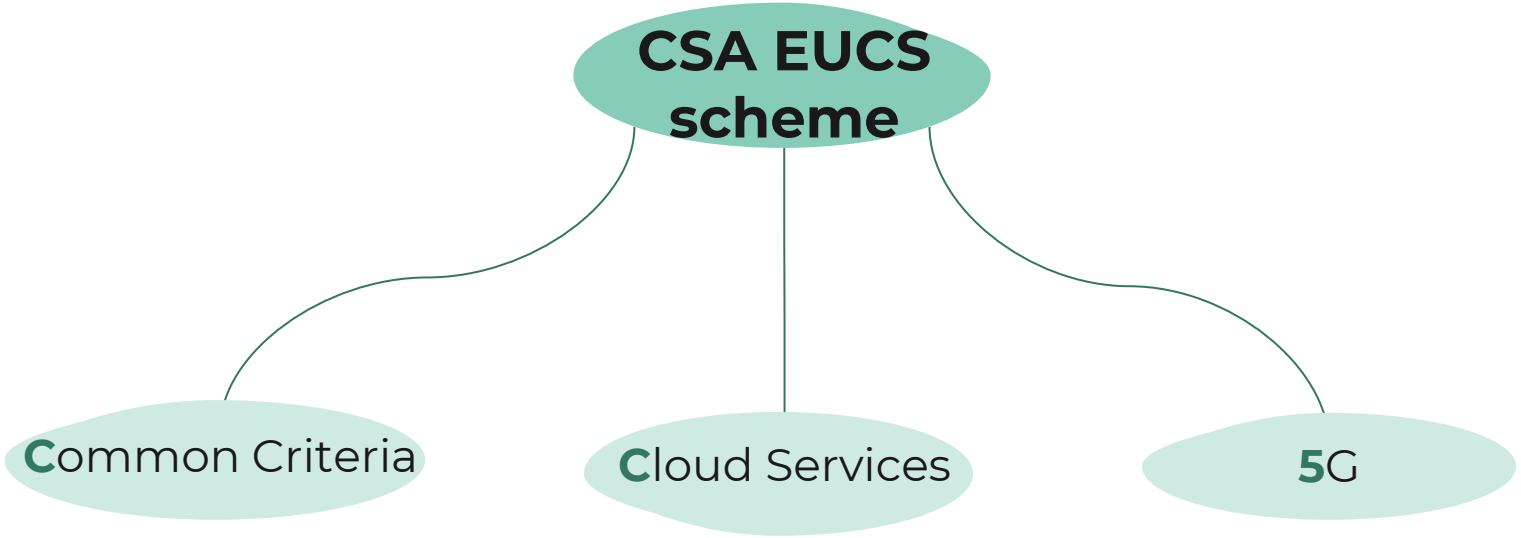
ax fined by ICO over data
that hit Britons

Credit rating agency Equifax is to be fined £500,000 by the Information Commissioner's Office (ICO) after it failed to protect the personal data of 15 million Britons.

Patching Requirements
through delegated certification

up-to-date software and hardware that don't contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

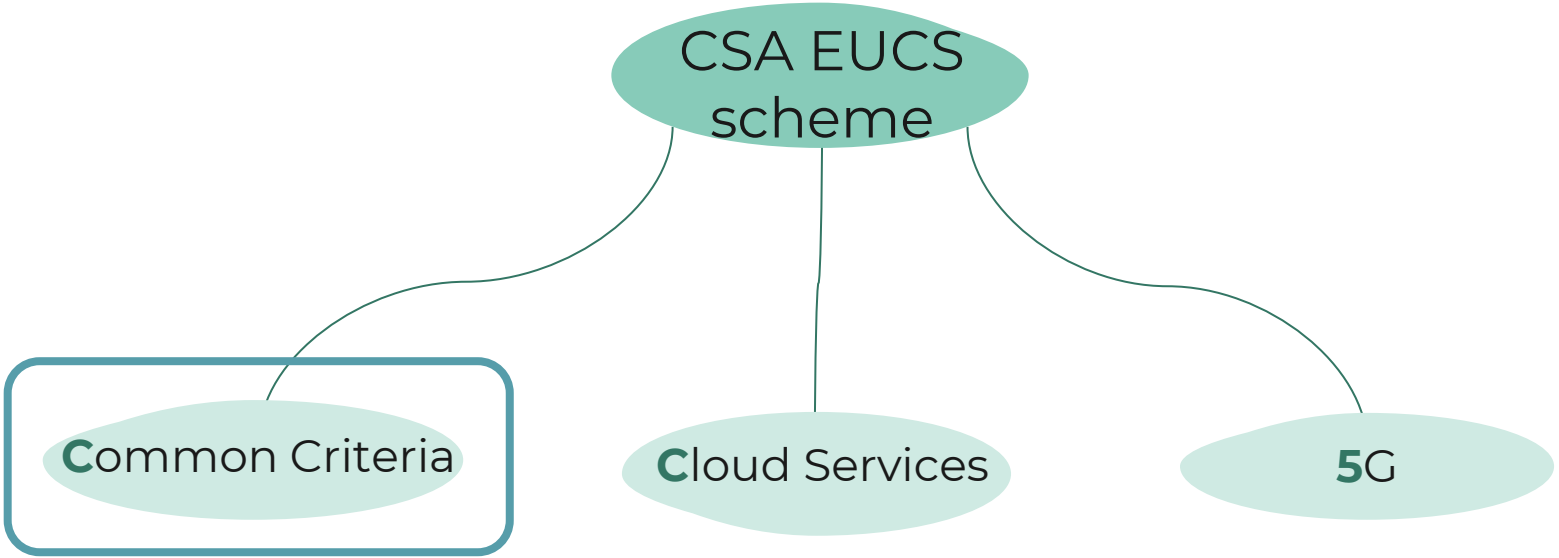
2019 CSA



Patching Requirements
through delegated certification

up-to-date software and hardware that don't contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

2019 CSA



Patching Requirements
through delegated certification

up-to-date software and hardware that don't contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.

2019 CSA

secure by default and by design, does not contain known vulnerabilities and includes the **latest security updates.**

2023 CSA Amendments for managed security services

- **C**ommon Criteria
- **C**loud Services
- **5**G

Specified Security Principles

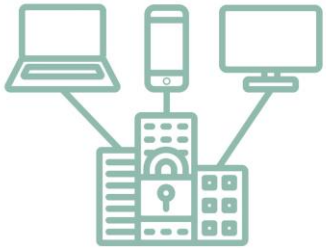
"shall take appropriate technical, operational and organisational measures to manage the risks posed to the security of network and information systems, **including:**"

Vulnerability handling

Cyber hygiene, including software & hardware updates.

Board liability

2022 NIS2



CRITICAL INFRASTRUCTURE

Sectoral Patching Requirements

2022 DORA

Cybersecurity for the financial sector

ICT Risk Management Framework

Policies for Patching & Updates

Governance & Control Framework

Horizontal Patching Requirements
with complementary certification & liability

2022 CRA – Product Security

Disseminate patches timely & free of charge

Handle vulnerabilities for the expected product lifetime

Essential cybersecurity requirements

Security by default and design

2022 Product Liability

including for a lack of software updates

Liability for cybersecurity defects in products

1 **Generic Security Requirements**

2 **Generic Security Requirements**
based on risk assessment & standards

3 **Specified Security Principles**

4 **Patching Requirements**
through delegated certification

5 **Sectoral Patching Requirements**

6 **Horizontal Patching Requirements**
with complementary certification & liability

Conclusions

Early stages

No obligations & focus on standards

Over time

Generic security requirements & standards

Near future

Specific patching requirements & responsibility

- Vertical obligation
- Horizontal obligation

Next Steps?

Interviews with +/- 30 CISOs on their patching policies

Questions?

E.M.Rooij@tilburguniversity.edu

THESEUS newsletter