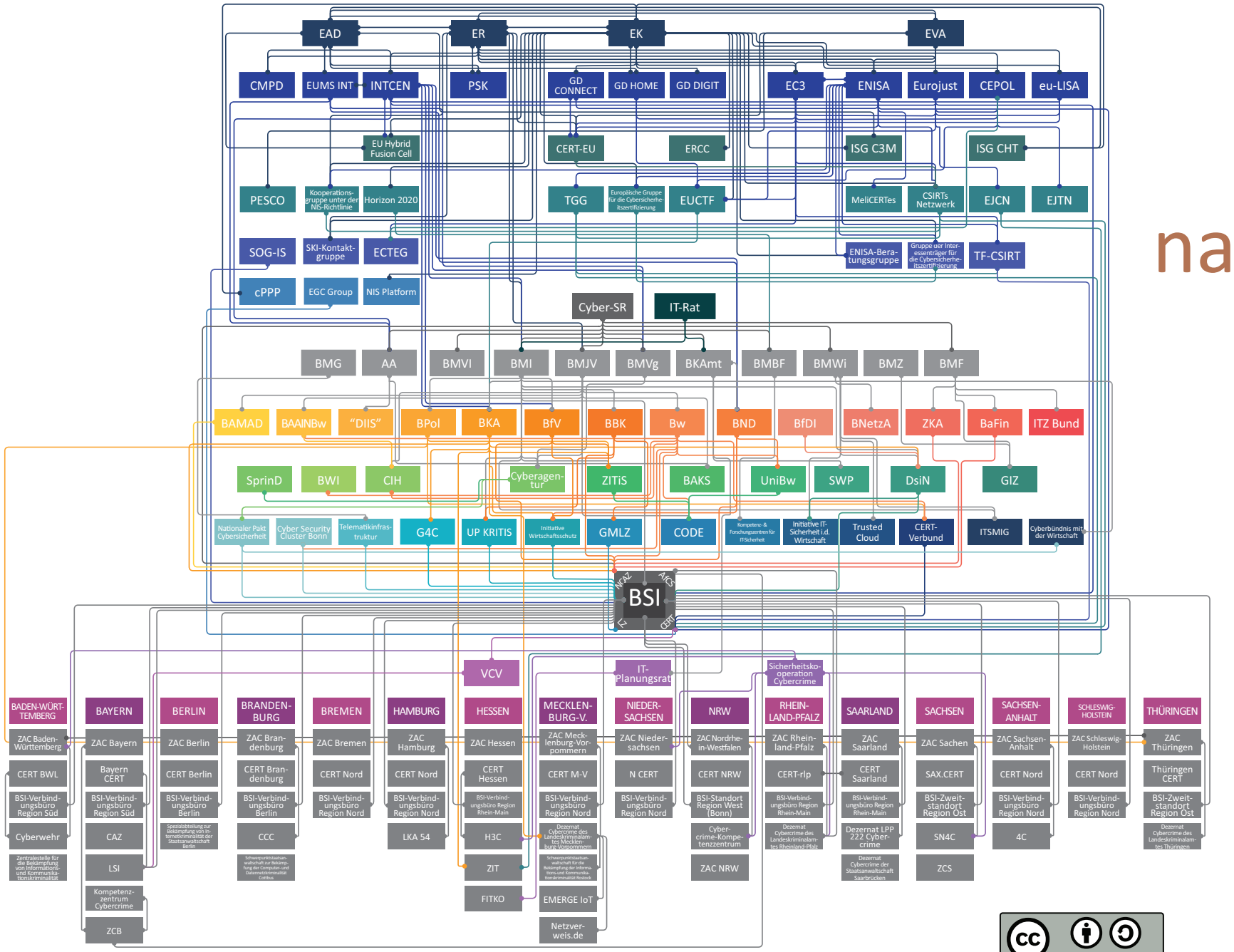
ICS Security – A European Perspective

Klaus Mochalski
CEO & Founder
km@rhebo.com

Rhebo

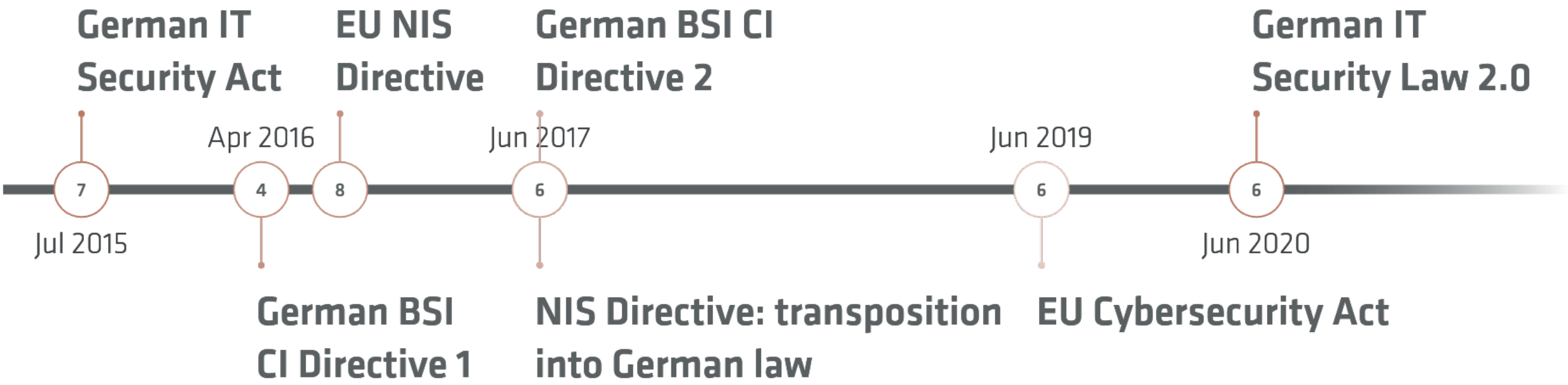
Industrial Network Continuity

The European context of the national German Cybersecurity Architecture



Stiftung Neue Verantwortung

European and German IT security legislation



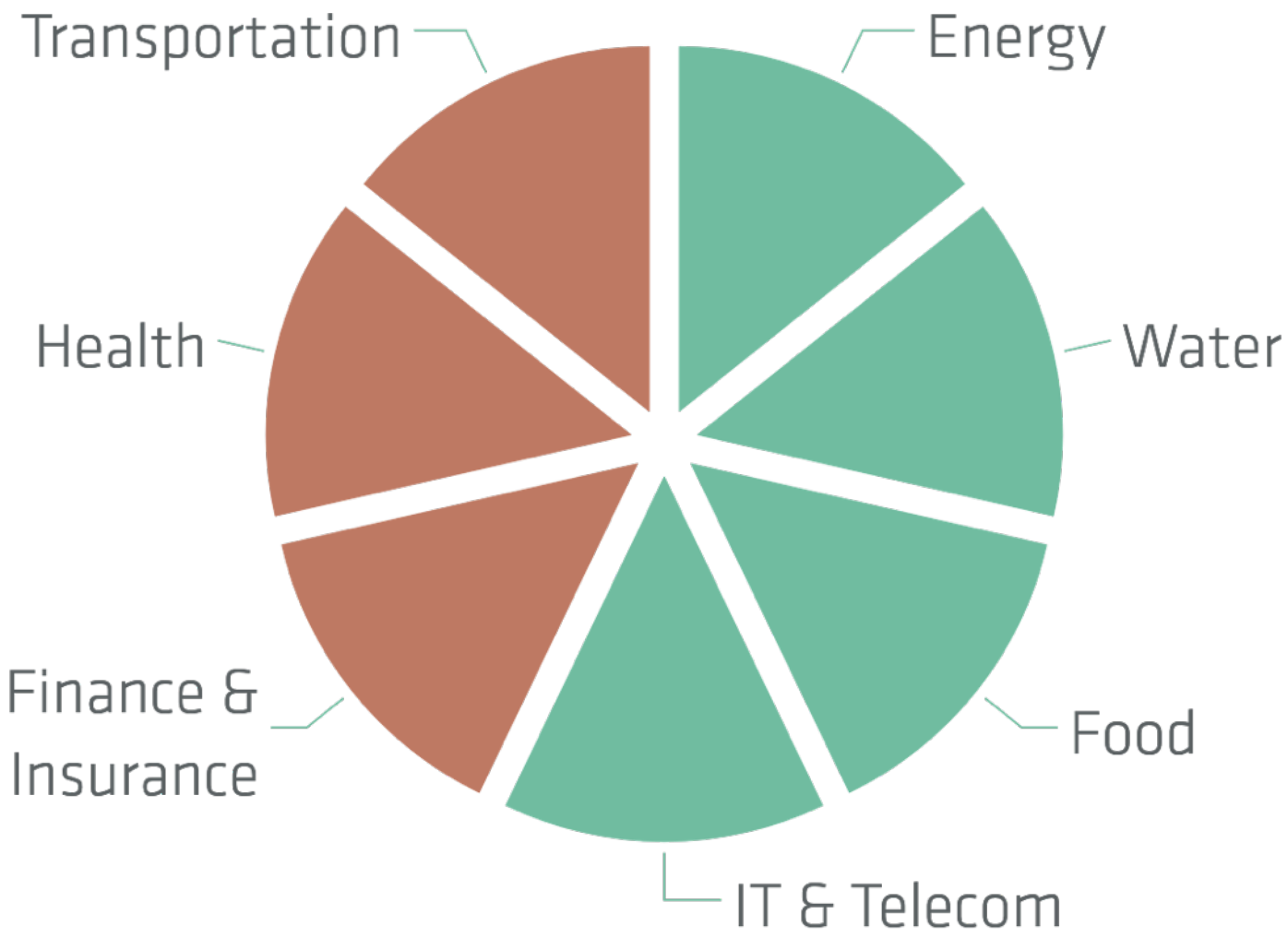
Regulations, standards & organizations that matter today in Germany, according to Rhebo

1. IT Security Act
2. BDEW whitepaper “Requirements for Secure Control and Tele-communication Systems”
3. IEC 62443
4. NAMUR WG 4.18 Automation Security
5. ENISA

IT Security Act (IT-SiG)

- applicable to critical infrastructures (CI)
- extended authority for the BSI (national cybersecurity authority)
- §8a: state-of-the-art requirement for IT security &
  ISMS incl. audit every two years
- §8b: reporting obligation for incidents that have caused
  or may cause a considerable disruption

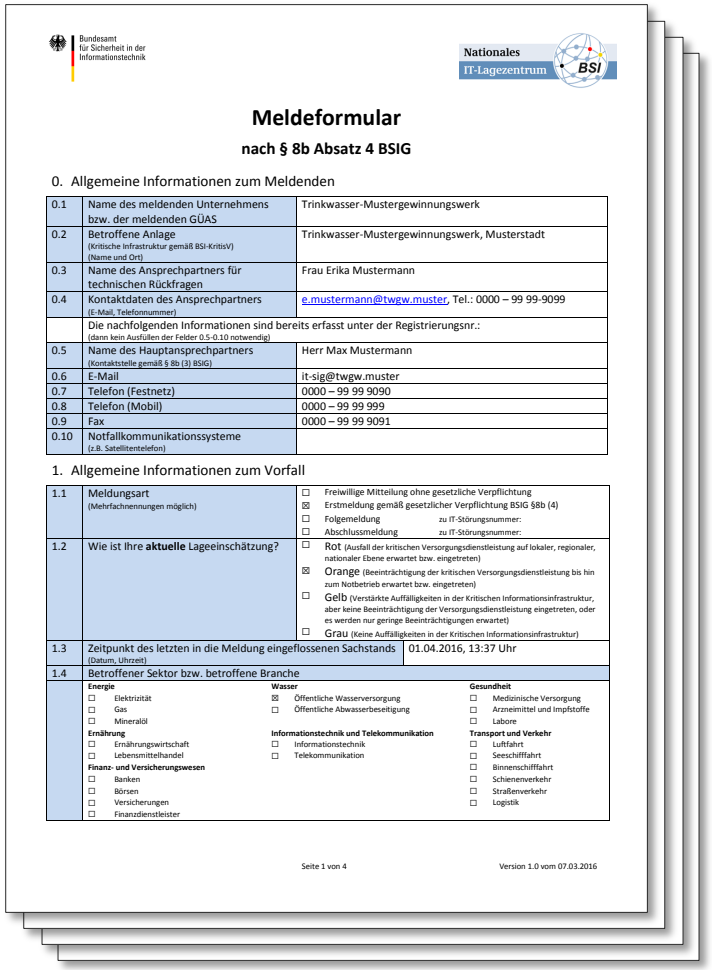
CI sectors & thresholds



500,000 supplied people, e.g.

- Power generation: 420 MW
- Power transmission & distribution: 3,700 GWh/y
- Gas supply: 5,190 GWh/y
- Crude oil: 4.4 Mt/y

We have the best forms: official BSI reporting form



Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

Meldeformular

nach § 8b Absatz 4 BSIG

0. Allgemeine Informationen zum Meldenden

0.1	Name des meldenden Unternehmens bzw. der meldenden GÜAS	Trinkwasser-Mustergewinnungswerk
0.2	Betroffene Anlage (Kritische Infrastruktur gemäß BSI-KritisV) (Name und Ort)	Trinkwasser-Mustergewinnungswerk, Musterstadt
0.3	Name des Ansprechpartners für technischen Rückfragen	Frau Erika Mustermann
0.4	Kontaktdaten des Ansprechpartners (E-Mail, Telefonnummer)	e.mustermann@twgw.muster, Tel.: 0000 – 99 99-9099
	Die nachfolgenden Informationen sind bereits erfasst unter der Registrierungsnr.: (dann kein Ausfüllen der Felder 0.5-0.10 notwendig)	
0.5	Name des Hauptansprechpartners (Kontaktstelle gemäß § 8b (3) BSIG)	Herr Max Mustermann
0.6	E-Mail	it-sig@twgw.muster
0.7	Telefon (Festnetz)	0000 – 99 99 9090
0.8	Telefon (Mobil)	0000 – 99 99 999
0.9	Fax	0000 – 99 99 9091
0.10	Notfallkommunikationssysteme (z.B. Satellitentelefon)	

1. Allgemeine Informationen zum Vorfall

1.1	Meldungsart (Mehrfachnennungen möglich)	☐ Freiwillige Mitteilung ohne gesetzliche Verpflichtung ☒ Erstmeldung gemäß gesetzlicher Verpflichtung BSIG §8b (4) ☐ Folgemeldung zu IT-Störungsnummer: ☐ Abschlussmeldung zu IT-Störungsnummer:
1.2	Wie ist Ihre **aktuelle** Lageeinschätzung?	☐ Rot (Ausfall der kritischen Versorgungsdienstleistung auf lokaler, regionaler, nationaler Ebene erwartet bzw. eingetreten) ☒ Orange (Beeinträchtigung der kritischen Versorgungsdienstleistung bis hin zum Notbetrieb erwartet bzw. eingetreten) ☐ Gelb (Verstärkte Auffälligkeiten in der Kritischen Informationsinfrastruktur, aber keine Beeinträchtigung der Versorgungsdienstleistung eingetreten, oder es werden nur geringe Beeinträchtigungen erwartet) ☐ Grau (Keine Auffälligkeiten in der Kritischen Informationsinfrastruktur)
1.3	Zeitpunkt des letzten in die Meldung eingeflossenen Sachstands (Datum, Uhrzeit)	01.04.2016, 13:37 Uhr
1.4	Betroffener Sektor bzw. betroffene Branche	

Energie
☐ Elektrizität
☐ Gas
☐ Mineralöl

Ernährung
☐ Ernährungswirtschaft
☐ Lebensmittelhandel

Finanz- und Versicherungswesen
☐ Banken
☐ Börsen
☐ Versicherungen
☐ Finanzdienstleister

Wasser
☒ Öffentliche Wasserversorgung
☐ Öffentliche Abwasserbeseitigung

Informationstechnik und Telekommunikation
☐ Informationstechnik
☐ Telekommunikation

Gesundheit
☐ Medizinische Versorgung
☐ Arzneimittel und Impfstoffe
☐ Labore

Transport und Verkehr
☐ Luftfahrt
☐ Seeschifffahrt
☐ Binnenschifffahrt
☐ Schienenverkehr
☐ Straßenverkehr
☐ Logistik

Seite 1 von 4 Version 1.0 vom 07.03.2016

Sections

1. Information about reporter
2. Information about incident
3. Description of disruption
4. Information about attack
5. Information about disruption of critcal service
6. Miscellaneous

BDEW whitepaper & XLS checklist

- “defines fundamental security requirements for control and telecommunication systems used for process control in the energy sector”
- “defines requirements for both individual components and systems / applications assembled from these components”
- important guideline for many (~ 50 %) of Rhebo’s utilities customers

oesterreichs energie.

bdew
Energie. Wasser. Leben.

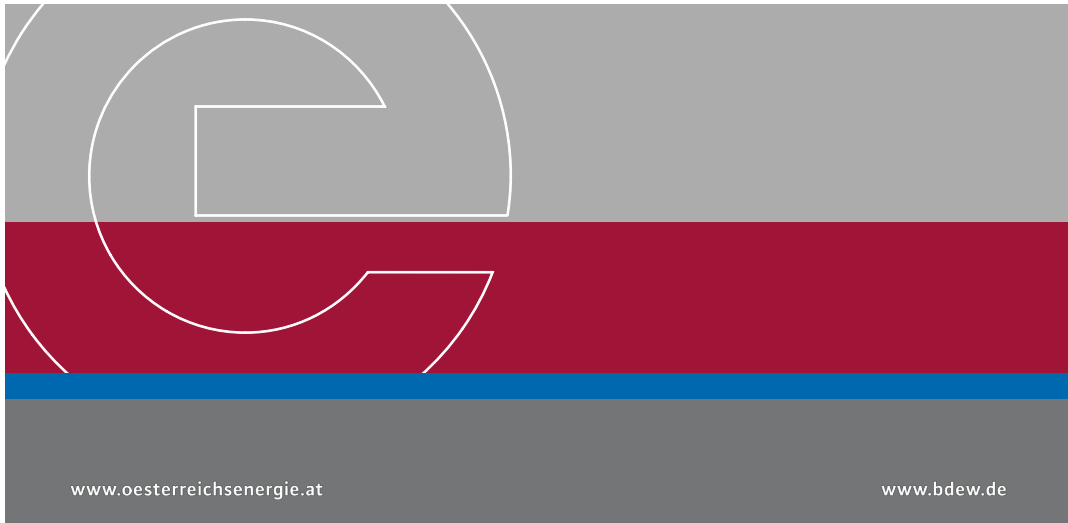
BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Oesterreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

Whitepaper Requirements for Secure Control and Tele-communication Systems

Completely revised version 2.0 05/2018:

Vienna/Berlin, 8th May 2018



Rhebo

PRACTICAL OBSERVATIONS

(Germany, Austria, Switzerland)

Awareness

- Compliance trumps conviction
- No German translation for “awareness”
- IT-SiG 1.0 first audit date (April 2018) made Rhebo’s year 0

Rhebo-observed security posture

Critical infrastructures:

- ICS/SCADA networks often well protected
- ISMS established
- general openness for OT monitoring & anomaly detection -> increasing footprint
- trust & data protection important (made in EU/Germany, GDPR)

Manufacturing:

- €€€ for incident response >> €€€ for prevention

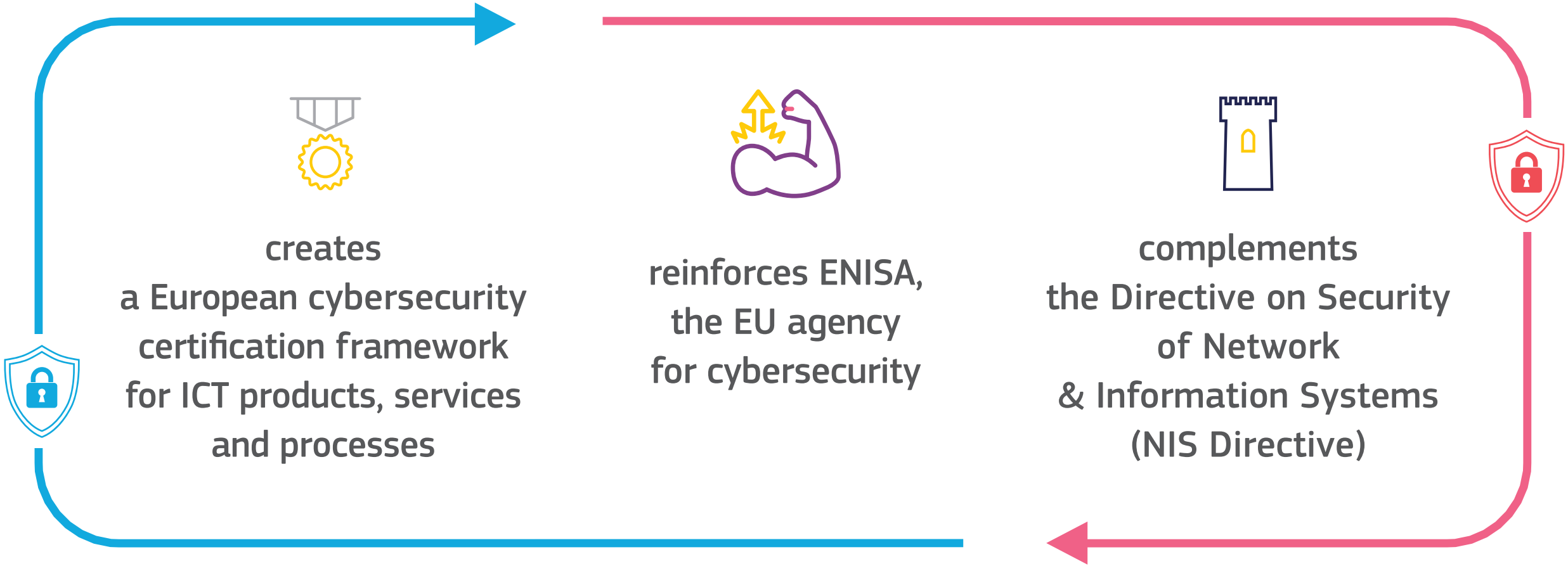
Relative occurrence of security issues

security issue	occurrence	security issue	occurrence
unsanctioned protocols	62.9%	intermittently active devices	11.4%
unsecure authentication	54.3%	unencrypted SMTP	11.4%
potential malware	54.3%	unencrypted Telnet	11.4%
vulnerable software	40.0%	ARP spoofing	11.4%
vulnerable operation system	37.1%	scan activity	11.4%
Internet communication	31.4%	IP fragments	8.6%
unencrypted FTP	25.7%	HTTP 403 (Forbidden)	8.6%
unencrypted HTTP	25.7%	Raspberry Pi	8.6%
self-assigned IP address	22.9%	unusual MAC addresses	8.6%
vulnerable firmware	22.9%	unusual inter-subnet communication	8.6%
manual HTTP login	20.0%	deprecated protocols	8.6%
new device at unusual time	20.0%	DNS bursts	5.7%
failed login attempts	14.3%	duplicate IP addresss	2.9%
vulnerable SSH version	14.3%	unusual Profinet communication	2.9%

Rhebo

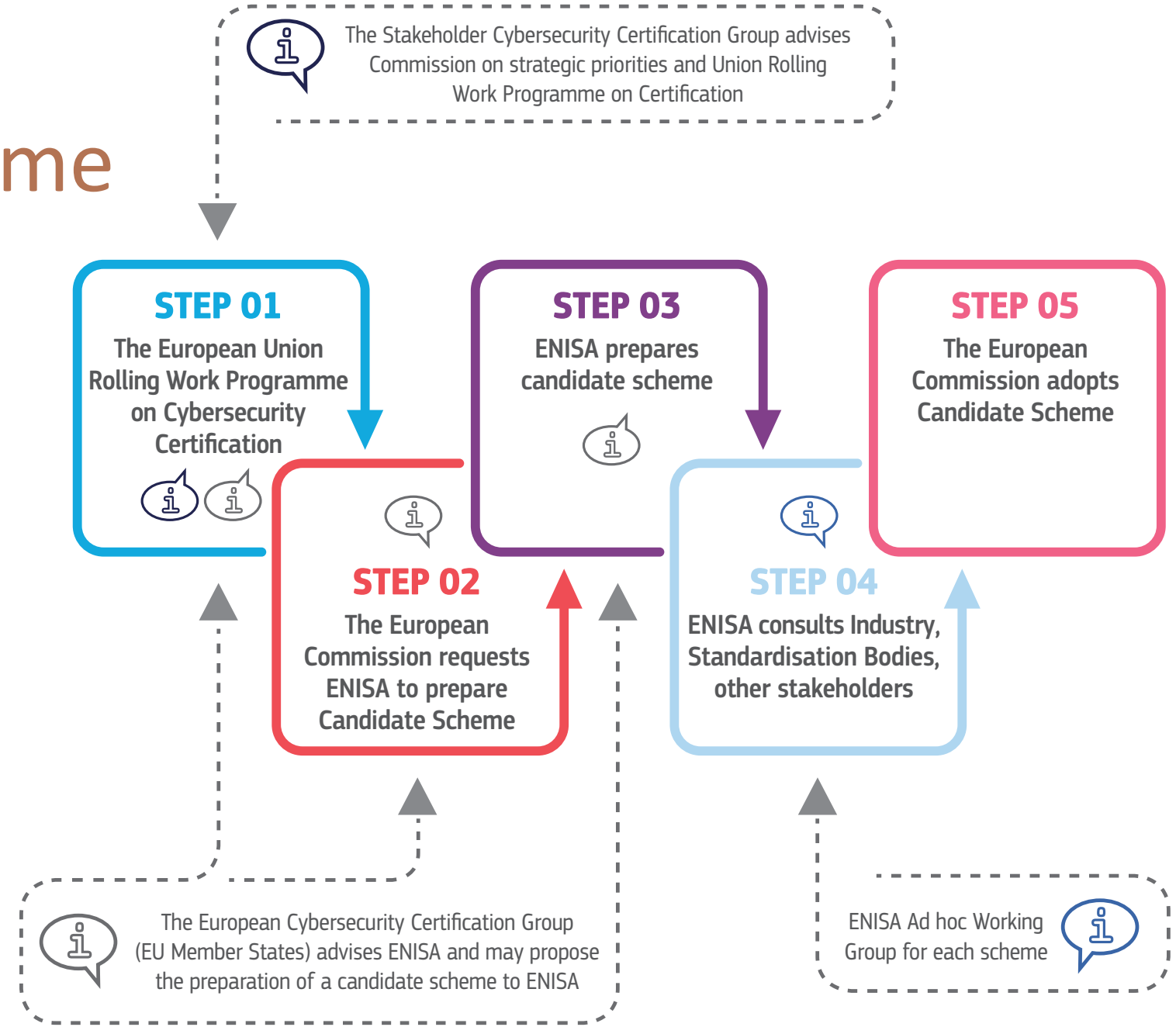
OUTLOOK

EU Cybersecurity Act entered into force 27 June 2019



Source: European Commission, https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-glance

EU cybersecurity certification scheme lifecycle



Source: European Commission, https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-glance

German IT Security Act 2.0

1.0 vs. 2.0 (preliminary)

- self-assessment of CI thresholds
- fines of up to € 100k
- IDS & SIEM only implicitly implemented as part of ISMS
- no hardware certification

- reversal of evidence for CI thresholds
- fines increased to GDPR levels (€ 20M or 4 % of annual revenue)
- IDS mandatory
- security certification for critical assets

Regulation trumps awareness

Rhebo

Klaus Mochalski
CEO
km@rhebo.com