



FERMA

Anticipating changes
Shaping the future

wtw

WEBINAR

**CYBER REPORTING STACK:
NAVIGATING THE EU
REQUIREMENTS**

12 February 2025

1. Speakers



Philippe Cotelle

Board Member, FERMA

Chair of the Digital Committee, FERMA



Laure Zicry

Head of FINEX Cyber, Western Europe



FERMA Anticipating changes
Shaping the future

wtw

Cyber Reporting Stack: Navigating EU requirements

- **Publication:** 4 October 2024
- **Download the report on FERMA's website:**



2. Purpose and Scope of the report

- Cyber risks are more than ever a threat to any organization
- Cyber reporting is a key aspect of the EU Cybersecurity Strategy, but requirements can be difficult to navigate
- Our report aims to help organisations to link the EU regulatory landscape to risk and insurance management



3. A brief overview of the regulatory landscape

General Data Protection Regulation (GDPR)

Reinforce the protection of the rights of EU citizens regarding the processing of their data (GDPR)

Regulation

Network and Information System (NIS2)

- Enhance the level of cybersecurity in the EU
- Introduce risk management measures and reporting requirements to entities from more sectors
- Set up rules for cooperation, information sharing, supervision, and enforcement of cybersecurity measures and enforcement

Directive

Digital Operational Resilience (DORA)

Strengthen the resilience of financial services in face of operational disruption from cyber incidents

Regulation

Cyber Resilience Act (CRA)

Safeguard consumers and businesses using products or software with digital elements with mandatory cybersecurity requirements

Regulation

All these regulations require notification to both Supervisory Authorities and if needed to individuals



3. A brief overview of the regulatory landscape




Accumulation of European legislations, all with distinct objectives and aims

= the burden of stacked regulations


Notification and Crisis Management concurrently



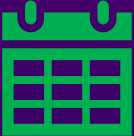
Complexity and stack of Cyber incident notification requirements




Different authorities




Different triggers



Different deadlines



Different content



Different sanctions

4. Case Study : Critical Infrastructure hit by a Ransomware Attack and a Data Breach

A €3 billion turnover company headquartered in France with a subsidiary in Luxemburg performing services in the health industry (hospitals or clinics), suffers a ransomware attack

NIS2

Applies to either public or private entities that

- 1. Fall under Annex I (sectors of High Criticality)** or Annex II (other Critical Sectors)
- 2. Are large enterprises:**
(i) Number of Employees greater than or equal to 250;
(ii) With a Turnover greater than or equal to €50m and/or an Annual Balance Sheet greater than or equal to €43m.
- 3. Provide their services or carry out their activities within the Union.**

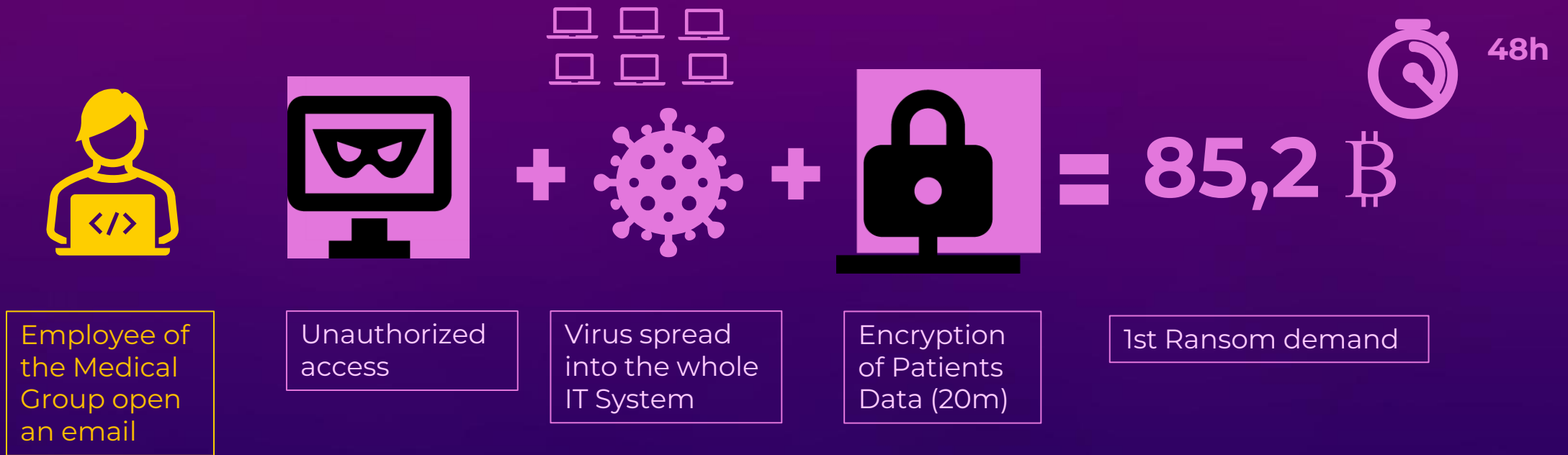
Annex I – Sectors of High Criticality

1. Energy
2. Transport
3. Banking
4. Financial market infrastructures
- 5. Health**
6. Drinking water
7. Wastewater
8. Digital Infrastructure
9. ICT service management (b to b)
10. Public administration
11. Space

GDPR

Applies to all companies either public or private, worldwide, that process personal data of EU Citizens.

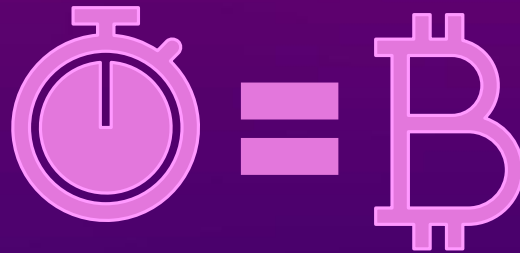
4. Case Study : Critical Infrastructure hit by a Ransomware Attack and a Data Breach



4. Case Study : Critical Infrastructure hit by a Ransomware Attack and a Data Breach



- Backups are also encrypted
- Negotiation with Hacker
- Attempt to decrypt the Data with Data Recovery Specialist



- First Countdown expired
- New Ransom demand



National Data Protection Authority



Notification letters sent to Data Subjects

4. Case Study : Critical Infrastructure hit by a Ransomware Attack and a Data Breach



Qualify the
incident



Notification
deadline



Supervisory
Authorities



Individuals



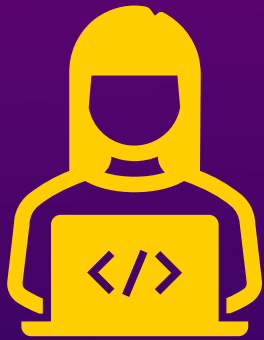
Sanction



Insurance

4. Case Study : Critical Infrastructure hit by a Ransomware Attack and a Data Breach

Qualify the incident



NIS2

Incident that has a significant impact on the provision of their services

An incident shall be considered to be significant if

- * it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
- * it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

GDPR

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4. Case Study: Critical Infrastructure hit by a Ransomware Attack and a Data Breach

Notification deadline



NIS2

24h for initial report,
72h for detailed report,
final report in 1 month

GDPR

Without undue delay and no later
than 72h.

4. Case Study: Critical Infrastructure hit by a Ransomware Attack and a Data Breach

Supervisory Authorities



NIS2

National competent authority
or
National CSIRT

GDPR

Data Protection Authority

4. Case Study: Critical Infrastructure hit by a Ransomware Attack and a Data Breach

Individuals



NIS2

Notification to Recipients : Entities shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services.

GDPR

Notification to Data subjects without undue delay when there is a risk of privacy

4. Case Study: Critical Infrastructure hit by a Ransomware Attack and a Data Breach ¹⁵

Sanction



Non-monetary remedies	Administrative fines	Criminal sanctions
<ul style="list-style-type: none"> • Compliance orders • Binding instructions • Security audit implementation orders • Threat notification orders to entities' customers 	<p>Essential Entities : Administrative fines of up to €10m or at least 2% of worldwide turnover, whichever amount is higher</p>	<p>For C-level management,</p> <ul style="list-style-type: none"> • Ordering that organizations make compliance violations public • Making public statements identifying the natural and legal person(s) responsible for the violation and its nature • And if the organization is an essential entity, temporarily ban an individual from holding management positions in case of repeated violations

Administrative fines
<p>Failure to comply with articles 33 and 34 can lead to "(...) administrative fines up to €10m, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (...)"</p>



4. Case Study : Critical Infrastructure hit by a Ransomware Attack and a Data Breach

Insurance



Crisis Management Costs

- IT Forensic costs
- Notification costs to Data subjects (patients), Data Protection Authority
- Notification costs to National CSIRT
- Call center costs
- ID monitoring costs
- Public relations costs
- Legal costs
- Mitigation costs
- Data restoration costs

First Party Coverages

- Business interruption
- Forensic accounting costs
- ICOW (Increased Cost of Work)
- Reimbursement of the ransom if paid

Third Party Liability

- Defence costs and indemnity to third parties (patients)
- Defence costs in front of the Data Protection Authority
- GDPR fines and penalties if covered
- NIS2 fines if covered

5. Practical Guidance for Risk Managers



Raise your profile

- Use this legislation to internally promote risk management's contribution to cybersecurity
- Position yourself as the **'orchestra conductor'** of risk management:
 - **Informing** about risks to adequately cover it in case of an incident,
 - **Collaborating** with key internal stakeholders to manage risks,
 - **Reporting** both internally and externally on any incident.

5. Practical Guidance for Risk Managers

Be involved in Cyber Risk Governance

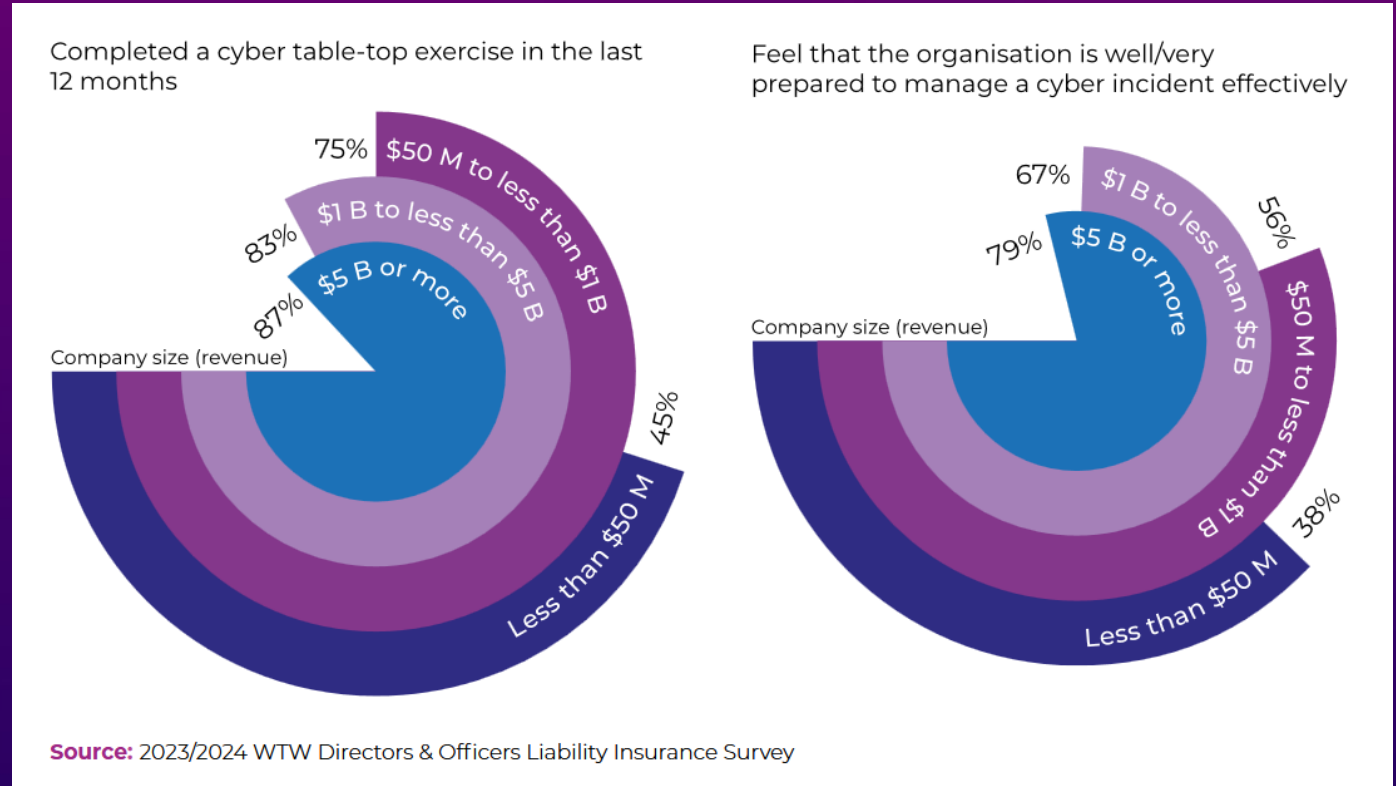
- Clear cyber governance structure is crucial
- Risk managers can play a central role
- Raise awareness on cyber risks within your organisations



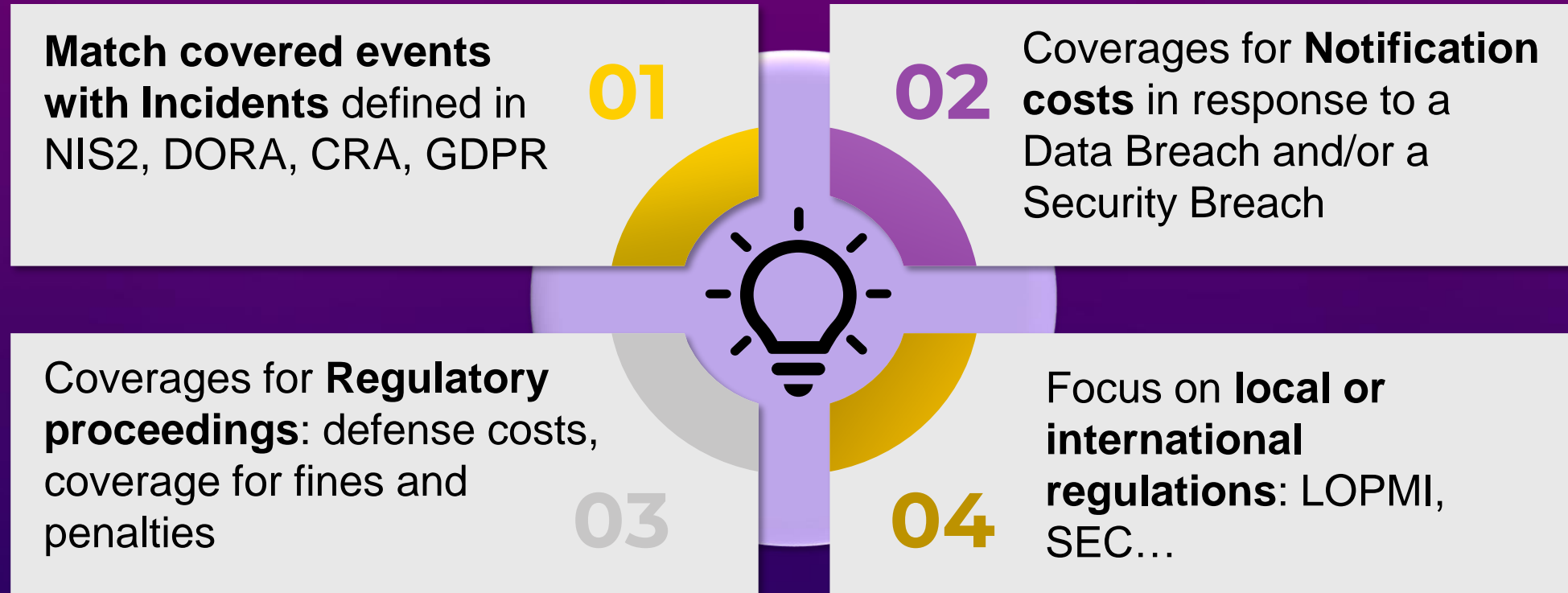
5. Practical Guidance for Risk Managers

Be prepared

- Have an incident response plan
- Conduct tabletop exercises



6. Insurance considerations



Recommendations to the EU

Strategic update

- ✓ Revise the EU Cybersecurity Strategy

Reporting stack

- ✓ Map all kinds of cyber-related reporting requirements, ransomware reporting requirements to identify areas of possible simplification
- ✓ Aim to reduce or simplify reporting requirements by 25%

Communication complexity

- ✓ Evaluate the concept of a “single point of entry” for cyber incident notification
- ✓ Give EU Member States guidance on how to streamline the various entities involved.

Role of the Risk manager

- ✓ Stimulate cyber risk management best practices, especially for the SME segment
- ✓ consider the insurance/risk transfer implications of future EU cyber legislation

Wrap-up



Are you ready?

Collaborate with key internal stakeholders to identify and assess new cyber notification requirements

Report both internally and externally any cyber incident related to new cyber security regulation

Make sure adequate coverages are included in your cyber insurance policy

Q&A



SAVE THE DATE!

FERMA's Next Webinar

- **Topic:** Global risk report 2025: the perspective of European Risk Managers and Internal Auditors
- **Date:** 17 February 2025, 16:00 to 17:00
- **Speakers:**
 - Lorraine Stack
 - Laurence Eeckman
 - Ann Brook
- **Moderator:** Daria Krivonos




LIVE WEBINAR

The Global Risk Report 2025

The perspective of European Risk Managers and Internal Auditors


Daria Krivonos
 CEO of the Copenhagen Institute for Futures Studies and FERMA Foresight Committee member


Lorraine Stack
 Managing Director and Risk Management Leader Europe at Marsh


Laurence Eeckman
 VP Group Risk Management at Atlas Copco AB and FERMA Board Member


Ann Brook
 Head of Technical Content and Research at the Chartered IIA

 17 February, 2025
  16:00 - 17:00 CET
  Zoom
 [REGISTER NOW](#)

SAVE THE DATE!

FERMA Seminar 2025

- Join the FERMA 2025 Seminar to explore the broadening horizon of **value chain** and what it means for risk management.

- **Date:** 23-24 October 2025

- **Place:** Hotel Kameha, Zurich, Switzerland

- **More information:**

www.ferma.eu/risk-management-events/



Contact us

FERMA - Federation of European
Risk Management Associations

Avenue de Tervuren 273, B12

1150 Brussels, Belgium

+32 2 761 94 32

www.ferma.eu

enquiries@ferma.eu

  @fermarisk

WTW

Laure Zicry

Head of FINEX Cyber, Western Europe

M + 33 (0) 6 73 92 89 16

laure.zicry@wtwco.com