CYBER REPORTING STACK: NAVIGATING THE EU REQUIREMENTS

FERMA Anticipating changes Shaping the future

with the support of wtw

Table of Contents

FOREWORDS

Charlotte Hedemark,
President of FERMA

Cyber risks are constantly evolving and have the potential to be catastrophic. Greater clarity about this risk and how to respond is, therefore, a major priority for regulators and governmental bodies.

To this end, the reporting of cyber incidents forms an important strand of the EU's Cybersecurity Strategy.
In recent years, the EU has progressively added more requirements for organisations to report on cyber incidents. These sit alongside myriad other reporting requirements at national and EU-levels. Outside of the EU, other jurisdictions such as the UK and the US also require disclosures about cyber risks and incidents.

FERMA believes that companies need a more streamlined and consistent set of requirements when it comes to reporting on cyber incidents. This reporting should help EU authorities, businesses and citizens all to better understand the cyber threat—but this will only work if it's easy, safe and secure for companies to provide information.
This white paper, which belongs to a growing body of work by FERMA on cyber risk, aims to help organisations link the EU regulatory landscape to risk and insurance management. It walks readers through a series of case studies to help companies understand when reporting requirements apply and how to handle them.
FERMA believes that a robust approach to understanding, responding to and managing cyber risk is strategically important for all organisations as part of a more strategic approach to dealing with the risks and opportunities of the digital economy.
Thank you to WTW for their collaboration in developing this report, which addresses a key area of the EU's policy agenda. We hope that it will give companies greater clarity about cyber incident reporting requirements and how those relate to the bigger picture of understanding this global threat.
We also hope that the knowledge derived from first-of-its-kind assessment will help European policymakers to streamline their approach to cyber incident reporting and lead to some simplification of reporting, enabling companies to devote a greater proportion of their resources and knowledge to assessing, managing and responding to this risk.

Top 5 risks in 2020	Top 5 risks in 2022	Top 5 risks in 2024
Cyber threats	Cyber threats (=)	Cyber threats (=)
Uncertain economic growth	Supply chain or disruption failure (▲)	Geopolitical uncertainties (▲)
Availability of key skills	Geopolitical uncertainties (▲)	Uncertain economic growth (▲)
Data fraud or theft	Uncertain economic growth (▼)	Talent management (▲)
Over-regulation	Over-regulation (=)	Data breach (▲)

Source: FERMA Global Risk Manager Survey Report 2024 (forthcoming)

Laure Zicry,
Head of Finex Cyber, Western Europe at WTW

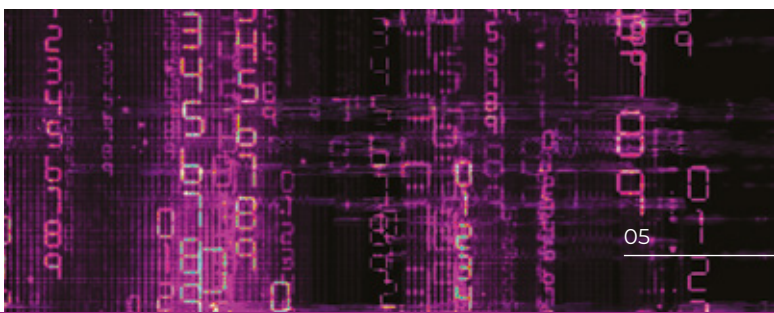
Even if companies implement 'best-in-class' and advanced cybersecurity measures, the risk of being hit by a cyber incident will never be reduced to zero. Properly managing cyber risks should be a priority for every company. Companies must also maintain confidentiality of their client's data, as well as their network security. Awareness, and more importantly, preparedness are fundamental when it relates to managing cyber risks.

The EU policy landscape is one of a host of variables that influence proper cyber risk management and this whitepaper, put together in collaboration with FERMA, aims to detail the complexity of cyber reporting requirements and how Risk Managers need to be prepared to face the duties imposed by a selection of EU legislation, together with key stakeholders at company.

The cyber incident reporting rules and requirements covered by this whitepaper deal with cross-functional issues and therefore need to be addressed by organisations accordingly.
The role of the Risk Manager is crucial to guarantee that all risks have been properly identified and that the optimal strategy has been applied to adequately protect their group.
Year after year, legislation after legislation... Even though every piece of the legislative puzzle make sense in building up cyber resilience, as well as protecting the data of European citizens (and more), today, we see a stack of Cyber reporting duties that companies need to comply with in case of a cyber incident.

For the same cyber incident affecting company, it must, in order to be compliant, notify various supervisory authorities, within very short but different deadlines. Further, there are constraints on the content and form of this cyber incident reporting, and potential pain points of being subject to not one, but as many sanctions as there is legislation. That is, even though the same company must deploy considerable resources to stop the attack, protect assets that were not impacted during the attack, restore its systems and data, and inform its customers and employees!

European companies are well aware that a cyber incident has the potential to paralyse their operations, and have therefore made significant efforts over the past years to improve their cyber security. Nevertheless, the various requirements within the range of European laws that touch upon cyber incidents challenges companies further still.



EXECUTIVE SUMMARY

In 2024, there can be no doubt that we face an increasing volume, complexity and scale of cyber threats. This report takes as its subject matter the growing onus on organisations to report on cyber threats and incidents a key part of the EU's Cybersecurity Strategy.

The Union's strategy has been, since 2020, intended to boost resilience and build collective capabilities to withstand and respond to cyber-attacks. FERMA is of the view that the EU has made considerable progress in its efforts to mitigate risks to the system, as well as bolster the capacity to respond. Nevertheless, we are concerned that since there is now a regulatory reporting stack emerging, the work required to comply with these requirements may divert resources from actually managing the risk.

Risk Managers play an important role in an organisation's approach to cybersecurity that goes far beyond complying with rules and requirements. Having a risk management approach to cyber risks means recognising that the cyber threat is unavoidable but also provides for a way of identifying, assessing, mitigating and managing those risks. Regulators also recognise the importance of risk management in the realm of cybersecurity; the Network and Information Security (NIS2) Directive even has specific articles outlining risk management measures.

Since penalties for non-compliance with the growing number of reporting requirements can be punitive, it is of the utmost importance that organisations operating in the European Union, and their risk management functions, gain clarity on which of these myriad reporting requirements are applicable to them, in which scenarios, and how they must respond.

This paper focuses on a selection of EU cybersecurity policies that require some form of incident reporting and is aimed at equipping Risk Managers with the tools they require to determine how to prioritise and respond to these requirements in a coherent way.

SELECTION OF EU CYBERSECURITY POLICIES

GDPR

- privacy and security law aimed at protecting the rights of individuals regarding the processing of their data
- in effect since 2018

NIS2

- aimed at boosting the cyber-risk preparedness and resilience of Member States by ensuring strategically important sectors have a culture of cybersecurity and robust incident response plans
- will update NIS1 in place since 2016

DORA

- aims at stregnthening the resilience of financial services entities in face of operational disruptions from cyber incidents
- will come into effect 17 January 2025

CRA

- aims to safeguard consumers and businesses using products or software with digital elements, with mandatory cybersecurity requirements on manufacturers and retailers
- expected to enter in force later in 2024

The various pieces of legislation examined in this paper contain different responsibilities and mechanisms for the reporting of cyber incidents.

The GDPR, for example, requires the data controller - the company or organisation - to notify the relevant data protection supervisory authority of a data breach without undue delay and, where feasible, not later than 72 hours after it has become aware of the breach. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Under NIS2, however, notification can be twofold, with entities required to notify their cyber security incident response team or relevant authority of an incident that has a significant impact on the provision of their services or, where appropriate to notify recipients of their services of significant incidents that might adversely affect the provision of those services.
These pieces of legislation also impose various sanctions for non-compliance, including fines, which may or may not be covered by insurance policies, depending on insurance coverage wording and the Member State in question.

This white paper outlines the policy landscape around cyber incidents and contains a series of case studies that illustrate various scenarios in which organisations would be required to report a cyber incident. The case studies also attempt to make a relevant link to insurance policies and are, overall, intended as examples to provide guidance about the possible reporting requirements that would apply in different scenarios, the timelines and process for reporting them, and the likely sanctions imposed in the case of non-compliance.
Lastly, this report holds significant policy relevance. While FERMA recognises the need for incidents to be reported, and for important information to be effectively relayed to those affected by a cyber-attack, we believe there are areas where the volume of reporting requirements, and the potential for overlap and duplication, place an overly onerous burden on organisations subject to an incident.

FERMA's vision for EU policymakers

Certain areas of these reporting processes should be simplified, in line with the European Commission's target of reducing reporting requirements by 25%. Industry also looks for further consideration of risk management in legislative matters.
FERMA therefore suggests:

- **the European Commission explore the potential for having a 'single point of entry' for cyber incident notification, as well as giving the EU Member States guidance on how to streamline processes and the number of entities involved.**
- **the European Cybersecurity Competence Centre and ENISA publish cyber risk management best practice in cooperation with the risk management community.**
- **the European Commission considers the insurance implications of any future EU cyber legislation when conducting Impact Assessments.**

CHAPTER 1

EU cyber incident reporting landscape

1 / Context: a selection of EU policies

Over the past 10 years, there has been a dramatic acceleration in the number of EU policy initiatives that concern the digital economy and cybersecurity.

From rules governing the use of personal data to the broader perspective of the resilience of critical entities and product design, the gamut of digital and cyber policy is vast. What unites these wide-ranging rules is a bid for transparency. Partly, this is due to a long-held belief in the EU that there is an insufficient common understanding of the main threats and challenges that surround EU Member States.

To address this 'information gap', the European Union has pursued a strategy in its policymaking of encouraging more sharing of information, built on a string of reporting requirements.
In the EU, the rules requiring organisations to keep record and report cyberthreats or attacks, and data breaches stem from legal acts - either a Regulation or a Directive. The former applies across all Member States as written, whereas the latter is generally a minimum harmonisation instrument that is transposed into national law allowing Member States to make some adjustments.

The landmark piece of legislation coming from the EU has undoubtedly been the General Data Protection Regulation ('GDPR'), heralded as the set of rules that institutionalises 'privacy-by-design'.
No less significant, however, has been the EU's first set of cybersecurity rules introduced in 2016 in the form of the Network and Information System ('NIS') Directive. Both of these are currently in force and in application.
Later in 2024, the update to NIS, i.e. NIS2, and in 2025, the first legislation on Digital Operational Resilience ('DORA') will come into play. While NIS2 expands the scope of NIS1 to encompass a much broader range of entities, DORA applies only to the financial services sector.
Further down the line, we expect to see the Cyber Resilience Act ('CRA') come into play. This Act will compel manufacturers to ensure cybersecurity-by-design in their production of digital goods.

Non-compliance with this stack of requirements will be met with sanctions. This is a cause for concern for many organisations. According to an annual survey conducted by WTW in 2024, regulatory breaches, and the threat of fines and penalties, are considered a significant risk for their organisation's business operations, either financially or reputationally – or both.

2/ Focus on significant EU notification requirements

Name	Type	In force	Transposition deadline	Applicable date
GDPR	Regulation	24 May 2016	Not applicable	25 May 2018
NIS1	Directive	8 August 2016	9 May 2018	10 May 2018
NIS2	Directive	16 January 2023	17 October 2024	18 October 2024
DORA	Regulation	16 January 2023	Not applicable	17 January 2025
CRA	Regulation	On the 20th day following that of its publication in the Official Journal of the EU. Expected to enter into force in 2024	Not applicable	Shall apply from [36 months from the date of entry into force of this Regulation]. However, Article 14 shall apply from [21 months from the date of entry into force of this Regulation].

Name	Scope	Requirements	Penalties
GDPR	All companies that process personal data of EU citizens	▪ Must notify relevant data protection authority in case of personal data breach without undue delay, not later than 72 hours ▪ and data subjects without undue delay	**1)** non-compliance with order by DPA will lead to a fine of €20 million or up to 4% of turnover, whichever is higher **2)** failure to comply with notification requirement can be met with a fine of either €10 million or up to 2% of annual turnover, whichever is higher
NIS1	Operators of essential services in specific industries to be identified by Member States.	▪ Must notify the competent authority or the cyber security incident response team (CSIRT) of incidents having a significant impact on the continuity of the essential services they provide, without undue delay	Member States to determine penalties to be effective, proportionate and dissuasive.
NIS2	This Directive defines two types of entities in Article 3: i) essential entities; and ii) important entities. Essential entities are generally of a certain (large) size.	▪ Entities must notify their CSIRT or relevant authority of any incident that has a significant impact on the provision of their services ▪ Where appropriate entities must notify the recipients of their services ▪ A communication must be made, where applicable, to the recipients of the entities services that are potentially affected by a significant cyber threat ▪ The timeline is based on three phases: 1) reporting without undue delay within 24 hours of becoming aware of significant incident in form of an early warning; 2) without undue delay, within 72 hours, an incident notification of the significant incident; 3) no later than one month after the submission of the incident notification a final report is due	**1)** Essential entities that infringe upon their reporting obligations are subject to administrative fines of at least €10 million or of a maximum of at least 2% of the total worldwide annual turnover, whichever is higher **2)** Important entities that infringe upon the reporting requirements are subject to fines of at least €7 million or a maximum of at least 1.4% of the total worldwide annual turnover
DORA	Financial under-takings and ICT third-party service providers	▪ Define, establish and implement an ICT-related incident management process ▪ Financial entities shall report major ICT-related incidents to the relevant competent authority—via notification template ▪ Time limits to be fixed by the ESAs	Member States shall lay down rules establishing appropriate administrative penalties and remedial measures. The penalties and measures shall be effective, proportionate and dissuasive.
CRA	**1)** Will apply to economic operators: manufacturers who develop or manufacture products with digital elements; **2)** will also apply to importers and distributors of such products	▪ Any actively exploited vulnerability contained in the product with digital elements simultaneously to the CSIRT and to ENISA ▪ A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements to CSIRT and to ENISA ▪ Manufacturers also have the obligation to inform the impacted users, and where appropriate all users, about the actively exploited vulnerability or a severe incident having an impact on security of a product, and where necessary about risk mitigation and any corrective measures that users can deploy to mitigate impact of the vulnerability ▪ There is a phased notification, 1st phase is within 24 hours of becoming aware of exploited vulnerability/severe incident; 2nd phase is to provide more information on the vulnerability/ incident, 3rd phase is within 14 days for the vulnerability detection as a final report, or within one month for the incident notification	**1)** Non-compliance with obligations on exploited vulnerability will be up to €15 million, or up to 2.5% of annual turnover, whichever is higher **2)** Non-compliance with reporting obligations for incidents shall be subject to fines of up to €10 million or up to 2% of annual turnover, whichever is higher

CHAPTER 2

Case studies

Walking through the obligations stemming from EU rules on reporting helps organisations understand the practical implications. It also might help to shift the mindset towards focusing on being prepared in the event of any incident. This chapter presents a series of practical case studies illustrating certain considerations for organisations when responding to the various reporting requirements.

The scenarios provide guidance on:

- Types of cyber incidents.
- The reporting obligations under existing regulations and examples of scenarios that would be triggered by upcoming regulations.
- The possible penalties for failing to comply.
- Insurance coverage to consider.

1/ Scenario 1: Critical Infrastructure hit by a Ransomware Attack and Data Breach

Cyber incident type: a €3 billion turnover company headquartered in France (main establishment within the meaning of GDPR, article 4(16)) with a subsidiary in Luxembourg performing services in the health industry (hospitals or clinics), suffers a ransomware attack.

An employee of the group in France receives an e-mail with a malicious link. When that employee clicks on the link, a group of hackers gains access to the IT systems ("unauthorised access") and to sensitive information (personal data related to health) of approximately 20 million patients. The hackers steal this data.
Because the company's IT systems are not segmented, the malware spreads into the entire IT system of the group (headquarters and subsidiaries).

Once they have access to the IT systems, the cyber criminals identify servers where personal data is stored, copy this data (personal data breach), and then encrypt this data.
Other employees at the health group inform the IT team that they cannot access any of the servers and are not able to work. After several hours, the malware has completely spread into the whole system, and the company can no longer perform any service (disruptive effect on the continuity of non-essential and of essential services).
In parallel, the employee who originally received the first e-mail with the malicious link discovers on his screen a ransom demand for 85.2 bitcoins (equivalent to $5 million at the time of writing) with a countdown timer (48 hours).
The board of directors at the healthcare group decides not to pay and to rely on backups. Unfortunately, the backups were also encrypted. The Chief Information Security Officer (CISO) decides to contact the hacker group to start negotiating the ransom while also contacting a Data Recovery Specialist to help with decryption of the data.
When the countdown expires, the hackers come back with a new ransom demand, threatening to disclose the data breach to the national data protection authority, as well as to the data subjects themselves (a two-stage attack)[1].

A few days later, the national competent authority contacts the Data Protection Officer (DPO) who realises that the 72-hour reporting deadline has been missed. The DPO also recognises that the violation of personal data entails a risk to the rights and freedoms of natural persons, and that this must be reported to the competent authority. Having failed to meet the 72-hour deadline set out in the GDPR, the group must notify the relevant regulatory authority of the personal data breach, giving reasons for the delay.

Reporting duties:

The company needs to comply with two European regulations, namely: NIS1 and GDPR.

1. › NIS1

The company is part of the health sector, which is mentioned in the directive, and in our scenario has been identified by France and Luxembourg as an Operator of Essential Services.

The incident has a significant disruptive effect on the group's network and information systems, and on the provision of its services that are deemed essential for the maintenance of critical societal activities.

Under the NIS1, the headquarters and the subsidiary must notify without undue delay their National Competent Authority or their CSIRT, of the incident having had a significant impact on the continuity of the essential services (article 14(3)). In order to determine the significance of the impact of an incident, the following parameters shall be taken into account:

Parameters to take into account to determine the severity of the impact of an incident:
(a) the number of users affected by the disruption of the essential service;
(b) the duration of the incident;
(c) the geographical area affected by the incident.

2. › GDPR

The group acts as a Data Controller under the GDPR.
Since the confidentiality of personal data has been compromised, the group has:

(a) to notify the personal data breach to the relevant Data Protection Authority where feasible, not later than 72 hours after having become aware of it (article 33 of the GDPR),
(b) to communicate to the data subjects without undue delay (article 34(1)) after it becomes aware of it.

In this scenario, the nature of data that has been stolen is health data (i.e. sensitive data such as date of birth, social security number, and medical results) so, the incident creates a privacy risk for data subjects.

Article 33 paragraph 3c states that communication to the data subjects is not required if it would involve disproportionate effort. In such an instance, there should instead be a public communication or similar measure whereby the data subjects are informed effectively of the situation. Under this scenario, the health company communicates with each of its 20 million patients individually. This incident should be documented in accordance with article 33(5).

Conclusion: The company must notify two authorities about the same incident (CSIRT and Data Protection Authority) and communicate with the 20 million affected patients.

Sanction

The group is subject to sanctions related to the non-compliance with the two Regulations.

1. › NIS1

As stated in article 21:
"Member States shall lay down the rules on penalties applicable to any infringements of national provisions adopted pursuant to this Directive, penalties provided for, shall be ***effective, proportionate and dissuasive."***

2. › GPDR

As stated in article 82.1:
"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. (...)"
Under this scenario, the group is accountable because of a lack of compliance with the GDPR and could be held liable for damage caused to third parties.
In addition to any indemnification that the health company may pay to third parties, the company is also subject to a potential penalty levied by the Data Protection Authority for not having notified them in due time and for not having put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
The maximum penalty is 2% of its previous year's total worldwide turnover with the minimum penalty being €10 million (art 83(4)).

Conclusion: Compliance with these obligations to report to different authorities within different timeframes adds an administrative burden on top of the management of the incident itself, resulting in significant costs for businesses.

Transferring the residual risk to an insurance contract is one of the purposes of a cyber insurance policy.

Insurance coverage to be considered

Cyber policies provide coverage for the consequences of a cyber-attack: those relating to the company's liability towards third parties, and those that have a direct impact on the company. A company should consider the following coverage options in order to address the scenario described:

Crisis Management Costs	▪ IT Forensic costs, ▪ Notification costs to Data Protection Authority and to the CSIRT ▪ Notification costs to Data subjects (patients), ▪ Hotline, ▪ ID monitoring costs, ▪ Public relations costs, ▪ Legal costs, ▪ Mitigation costs, ▪ Data restoration costs,
First Party Coverages	▪ Business interruption, forensic costs, ▪ ICOW (Increased Cost of Work), ▪ Reimbursement of the ransom if paid
Third Party Coverages	▪ Defence costs and indemnity to third parties (patients), ▪ Defence costs in front of the Data Protection Authority and applicable GDPR fines and penalties if covered

Additional consideration

As this first scenario concerns an incident that affected IT systems based in France, it is important to highlight the existence of a French regulation that came into force on April 24, 2023.
Article 5 of the LOPMI (Orientation and Programming Law of the Ministry of the Interior) marks the entry of cyber risks into the French insurance code and makes it compulsory for any victim of an attack on an automated data processing system to report to the competent authorities (police, *gendarmerie,* or the public prosecutor) within a short timeframe in order to be compensated by any insurance policy.

Requirement of the French Insurance Law

Art. L. 12-10-1 -The payment of a sum pursuant to an insurance contract clause covering compensation of an insured for losses and damages caused by an attack on automated data processing system [per Articles 323-1 to 323-3-1 of the Criminal Code] (IT system) is subject to the filing of a complaint by the victim with the competent authorities no later than 72 hours after the victim becomes aware of the attack. This article applies only to legal entities and to natural persons in the context of their professional activity.

This new reporting duty is in addition to the reporting duties linked to the GDPR and the NIS.

2/ Scenario 2: Malicious data breach affecting a financial institution

Let's assume that we are in July 2025 to attempt to understand what impact DORA and NIS2 will have on this scenario.

Please note that the reporting duties that we describe below are the ones applicable at the time of writing. The two regulations are in force but still not applicable, so some further changes could apply to the reporting duties. Additional elements of clarification will also be provided by the transposition of the directive into local law by the Member States.

Cyber incident type: a €2 billion turnover credit institution company based in the European Union with more than 7,000 employees is subject to a sophisticated hack.

Not only do hackers gain unauthorised access to the credit institution's IT systems, but also to the personal data of five million customers (i.e. name, address, email address, phone number and banking details). IT systems are also no longer accessible.
One of the credit institution's employees noticed a database query being run using his their credentials. The employee stopped the query and reported this issue to the credit institution's IT security Team.
Confidentiality of data is a subject taken very seriously by the group which implemented encryption measures to better protect it against a violation of the confidentiality of the data.
The Data Protection Officer (DPO) of the credit institution was immediately informed and notified the relevant Data Protection Authority.
The most important IT systems that supports major functions of the credit institution were still unavailable four days after the attack, despite considerable efforts by the IT security team.
The credit institution was no longer able to serve clients, and employees were not able to access systems.

Reporting duties

As this scenario takes place after DORA and NIS2 have come into application, the reporting duties that the credit institution must comply with are the following.

1. › NIS2

The company is a credit institution that falls within the sectors of high criticality defined in Annex 1 of the NIS2. It is large in size, and therefore considered an essential entity according to article 3 of NIS2 Regulation.

However, article 1(2) of DORA, Article 4 "Sector-specific Union legal acts" of the NIS2 Directive provides that:
1. Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive, including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.'"

Conclusion: The credit institution has no reporting duties related to the NIS2 Directive. Only the DORA requirements outlined below need to be met.

2. › DORA

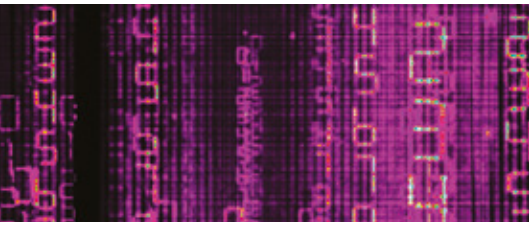
The DORA regulation applies to an exhaustive list of sectors including credit institutions, as mentioned in article 2 (1(a))[4] .
The credit institution company would need to report major ICT-related incidents to the local relevant competent authority.
The cyber-attack suffered by the credit institution constitutes a major ICT-related incident, classified as one that has a high adverse impact on the network and information systems that support critical or important functions of the credit institution.
The notification processes that must be conducted are:

- An initial notification and reports to the competent authority
- An intermediate report
- A final report

Deadlines to report the incidents will be set by the European Supervisory Authorities through its Joint Committee, in consultation with ENISA and the ECB.
In addition to the initial, intermediary and final reports, if the incident may have an impact on the financial interest of its clients, the credit institution must inform its clients about the incident and any measures that have been taken to mitigate adverse effects, without undue delay and as soon as it becomes aware of the incident.
Due to the large number of clients affected (five million), the credit institution may delegate the dissemination of such information to its clients to a third party, pursuant to article 19(5) of DORA.

3. › GDPR

The credit institution must also comply with the GDPR by notifying the relevant Data Protection Authority, where feasible, not later than 72 hours after having become aware of the incident (article 33 of the GDPR),



No communication to the data subjects (clients) is required because the data was encrypted.
Article 34(3) of the GDPR provides for cases where the communication to the data subject shall not be required:
"(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption".
This incident should be duly documented in accordance with article 33(5).

Sanction

1. › DORA

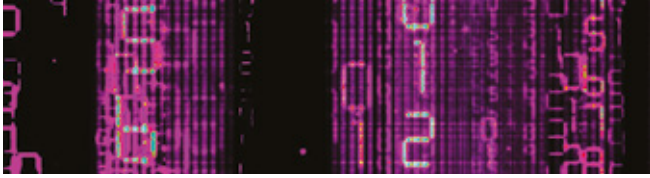
DORA leaves it up to the Member States to provide for appropriate penalties.

2. › GDPR

According to our scenario, the Data Protection Authority likely will not fine the credit institution after having received all relevant documentation and proof that there was no risk to the rights and freedoms of natural persons.

Insurance coverage to be considered

Crisis Management Costs	▪ IT Forensic costs, ▪ Notification costs to Data Protection Authority, ▪ Notification costs to data subjects (clients and employees), ▪ Hotline, ▪ ID monitoring costs, ▪ Public relations costs, ▪ Legal costs, ▪ Mitigation costs, ▪ Call centre, ▪ Data restoration costs
First Party Coverages	▪ Business interruption, ▪ ICOW (Increased Cost of Work)
Third Party Coverages	▪ Defence costs and indemnity for damage caused to clients and employees because of the Data Breach. ▪ Costs incurred by the insured to face the enquiry of the DPA, for example: lawyer, cyber security expert costs, etc. ▪ Defence costs for appearance before the local relevant competent authority, ▪ and Fines and Penalties where applicable after DORA is adopted.



3/ Scenario 3: Software supply-chain attack

Cyber incident type: a €1 billion turnover German company, a leader in software to assist and support Human Resources services for employees (i.e. management of pay slips and salary payment, bank data, health and benefits) is hit by a cyber-attack.

Hackers managed to identify a vulnerability in a piece of software that had not been detected by the company's IT security team. They actively exploited this vulnerability, not only gaining access to the company's IT system (which uses its own product) but also to the IT systems of all its clients in the European Union and worldwide. All companies in European Union or elsewhere in the world that were using this software were targeted by the hackers, who managed to access their IT systems and steal hundreds of gigabytes of data related to their employees and, in some cases, even to their families.

Unfortunately for the German company, all data relating to employees and their families was not encrypted.
The company conducted an internal investigation, supported by an external IT forensic firm, that determined that the hackers had encrypted and exfiltrated data (log files showed data flow to the outside during the attack period).

A couple of days after the event, several clients disclosed to the German company that they had suffered an attack. Companies affected by the vulnerability were no longer able to send employees their pay slips nor pay their salaries. The company quickly came to the following conclusion: malicious actors had exploited the exposed vulnerability and accessed its clients' systems without permission.

Following this disclosure, the IT security team at the company developed a patch to correct the vulnerability and released this patch publicly. It also informed all its clients about both the existence of the vulnerability and the related patches.

Reporting duties:

1. › CRA

The German company is a manufacturer of a Product with Digital Element (PDE). It sells this product to companies of all sizes within the European Union and worldwide.

According to the CRA:
Article 3(13) "manufacturer' means a natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under its name or trademark, whether for payment, monetisation or free of charge".
Article 3(1) "product with digital elements" means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately".
Article 3(2) "remote data processing" means data processing at a distance the software for which is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions."
The German company needs to first notify the CSIRT of this exploited vulnerability.
The vulnerability exploited by the hackers allowed them to access personal data and resulted in the product not being able to perform as intended. As the incident can also be qualified as a severe incident, having an impact on the security of the product with digital elements, another notification need to be made because the cyber-attack on the product is an "incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions" - as companies were no longer able to send employees their pay slips nor pay their salary.

Reporting duties

1. Make an early warning notification, indicating, where applicable, the Member States in the territory of which the manufacturer is aware that its product with digital elements has been made available without undue delay and in any event within 24 hours of becoming aware of the actively exploited vulnerability/becoming aware of the severe incident having an impact on the security of the product,
2. Upon the request of the CSIRT designated as coordinator, send an intermediate report on relevant status updates.
3. Notify this exploited vulnerability to the CSIRT designated as coordinator and to ENISA (article 14(1)).
4. Notify the incident qualified as a severe incident having an impact on the security of the product with digital elements (that it becomes aware of) simultaneously to the CSIRT designated as coordinator and to ENISA (article 14(3)).
   The necessary steps to follow for these two notifications are explained the Appendices to this white paper.
5. Inform the impacted users of the product with digital elements, about the actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements and, where necessary, about risk mitigation and any corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident (article 14(8)).

Note: the reporting duties that we describe above are those applicable at the time of writing. The CRA regulation has not yet been published to the OJEU.

1. › GDPR

By gaining access to the software also used by the company itself, the hackers were able to steal personal data of employees of the German company and their families. This constitutes of a Data Breach as it can be qualified as a violation of the confidentiality of personal data.
There is one notification and one communication to make:

- (a) to notify the personal data breach to the relevant Data Protection Authority where feasible, not later than 72 hours after having become aware of it (Article 33 of the GDPR),
- (b) to communicate to the data subjects without undue delay (Article 34-1).

In this scenario, the type of data stolen is personal data and financial data (date of birth, bank account) meaning that the incident creates a privacy risk for data subjects.
Note that article 33 paragraph 3c states that the communication to the data subjects is not required if it would involve disproportionate effort. In such a case, there should instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
For this scenario, we will imagine that the software company opts to communicate individually to each of its employees and their families.
This incident should be duly documented in accordance with article 33(5).

Sanction

1. › CRA

At the time of writing, the CRA has yet to be transposed into national law and so the relevant penalties are yet to be defined by Member States. Nevertheless, based on the information available, it is worth noting that any company failing to comply with notification duties is subject to administrative fines of up to €15 million or, up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher (article 64(2)).

2. › GDPR

As stated in, article 82.1:

"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. (...)"

In this scenario, the group has failed to comply with the GDPR and may be liable for damage caused to third parties.

It is worth noting that the German company may also be fined for not having put in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Article 32), for up to 2% of its previous year's total worldwide turnover or a minimum of €10 million (Article 83(4)).

Insurance coverage to be considered

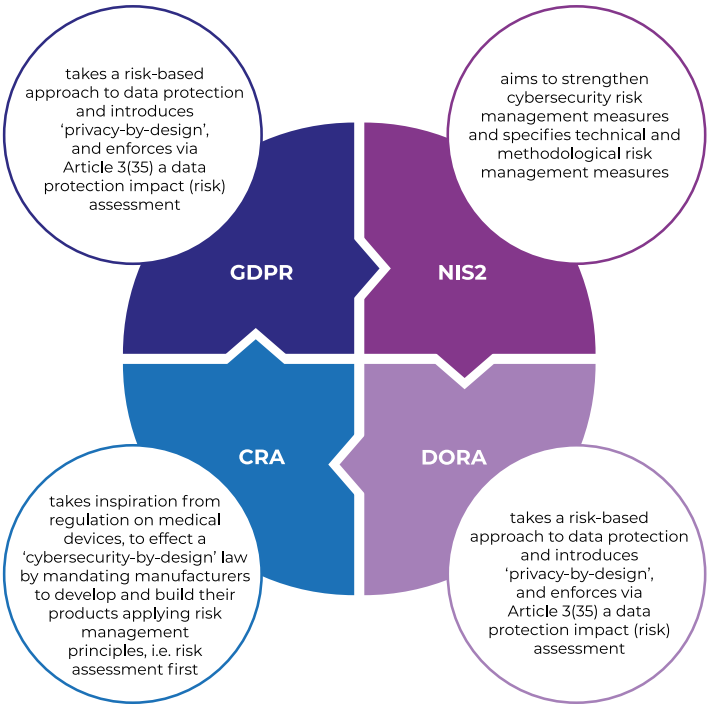
Crisis Management Costs	▪ IT Forensic costs, ▪ Notification costs to data protection authority, Notification costs to data subjects, ▪ Notification Costs to CSIRT and to ENISA, ▪ Hotline, ▪ ID monitoring costs, ▪ Public relations costs, ▪ Legal costs, ▪ Mitigation costs, ▪ Call centre, ▪ Data restoration costs
First Party Coverages	▪ Business interruption, ▪ ICOW (Increased Cost of Work)
Third Party Coverages	▪ Defence costs and indemnity due to damages caused to Employees and their Families because of the Data Breach. ▪ Defence costs in front of the Data Protection Authority and applicable GDPR fines and penalties if covered, ▪ Defence costs for appearance before CSIRT and to ENISA and Fines and Penalties where applicable after the CRA is adopted.

CHAPTER 3

Practical guidance for Risk Managers

Risk Managers are well-placed to help organisations confront cyber risks and the mounting reporting requirements in a strategic manner, which goes beyond complying with the rules. Companies that can better manage cyber threats will also be better equipped to meet the related regulatory requirements.

Furthermore, a certain risk management logic can be found at the heart of each piece of legislation covered in this report. However, an explicit link between cybersecurity and data protection to the role of Risk Manager is missing in the legislation.



The first piece of guidance to Risk Managers is to familiarise themselves with these important pieces of legislation and use them internally to promote the important role risk management plays in their organisation's approach to cybersecurity and reporting on cyber incidents. As a first example, NIS2 has a linked implementing regulation which specifies technical and methodological requirements of cybersecurity risk management measures.

Put another way, NIS2 explicitly links risk management to strengthening cybersecurity, incident management and oversight measures—making risk management central to achieving the aims of the law. Risk Managers should therefore be a centrifugal force in their organisation's approach not only to comply with NIS2, but also in their overall cybersecurity measures.

The remainder of this section presents a set of guiding principles for Risk Managers and risk management that relate to cyber incident reporting, based on the policy landscape as well as the lessons drawn from the case studies to illustrate the practical implications. In addition, it is important to cover the role of insurance in this area.

1/ Risk Managers' role and duties related to cyber incident reporting

The Risk Manager's role and duties in incident reporting do not start when the cyber incident occurs but well before it.
The cyber incident reporting rules and requirements covered by this white paper deal with cross-functional issues and therefore need to be addressed accordingly by organisations.
The role of the Risk Manager is crucial to guarantee that all risks have been properly identified and that the best strategy has been applied to adequately protect their organisation.
Furthermore, NIS2 and DORA specifically require organisations to implement and document risk management processes.
Risk management is not just the responsibility of Risk Managers but of everyone within an organisation. Risk Managers' roles are essential to identify, assess and develop the right strategies to transfer risk and put measures in place in case of an incident. To do this, they need to work closely with key stakeholders to properly manage all the legislative requirements in the

event of an incident. Within this context, the Risk Manager can essentially play the role of an 'orchestra conductor', with duties as follows:

- To inform about any risk in order to adequately cover it in case of an incident.
- To collaborate with key internal stakeholders to manage risks and act appropriately when risks arise.
- To report both internally and externally any incident, where applicable.

OTHER KEY STAKEHOLDERS

When it comes to cyber risk, the key stakeholder in this cooperation is the Chief Information Security Officer (CISO) – or equivalent – who is in charge of Information security and IT security. CISOs are the first to be informed and involved in the event of an incident. Close cooperation between CISO and Risk Manager appears to be the best practice for any company to deal with its risks, reputation and clients.
The Data Protection Officer (DPO) is another important person to deal with and one who must be involved when any incident involving data theft or privacy breach needs to be notified to the DPO. As we have described in our white paper, the DPO is the lead actor for notifying the data breach to the Data Protection Authority.
The Risk Manager must also work closely with Internal Audit and Compliance to make sure that the company is compliant with all applicable regulations when managing risks and also when an incident occurs.

Last but not least, Risk Managers will also have to inform the Board of Directors - with the support of the CISO - of the organisation's obligations with regard to the rules imposed by these regulations. Boards of Directors should be well aware that a cyber incident may put the company at risk both financially and reputationally. In the most recent WTW Directors and Officers Survey, Risk Managers were asked the following question: *"How important are the following risks for the directors and officers of your organisation (whether financially or reputationally)?"*
After Health and Safety (which ranks first following the 2020 pandemic), for 79% of the respondents, cyber-attacks (including cyber extortion) were deemed important, followed by Data Loss for 78% of respondents, and Artificial Intelligence/Machine Learning for 48% of respondents.

Directors and Officers are at the forefront of Cyber risk management since in the event of a cyber-attack they may be held personally liable.
It is worth noting that Chapter II, Article 5(2a) "Governance and Organisations" of DORA states that:
"2. The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1)."
For the purposes of the first subparagraph, the management body shall:
a) bear the ultimate responsibility for managing the financial entity's ICT risk;"

2/ Good practice guide to work towards better cyber incident reporting

Being ready to notify, communicate or inform within the framework of regulatory obligations requires preparation. Here are a few key pointers, and common pitfalls to avoid, in incident reporting.

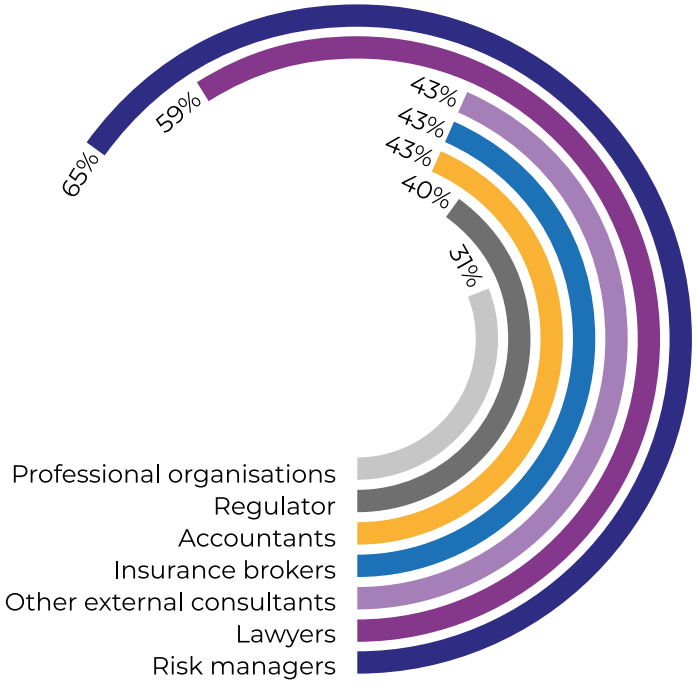
Cyber risk governance

Ensuring there is a clear governance structure in place is a vital pre-requisite to managing the reporting burden. However, there is not a single solution that works for every organisation.

Nevertheless, cyber risk governance should be clear and help to reassure all involved that the organisation has the right people, structures and processes in place.
The role of Risk Manager can be central to this, as has been shown in the 2017 FERMA & ECIIA 'At the junction of corporate governance & cybersecurity' report.
As with other risks facing organisations, informing the Board of Directors on cyber security and changes to the cyber-threat landscape is a core duty of the Risk Manager.

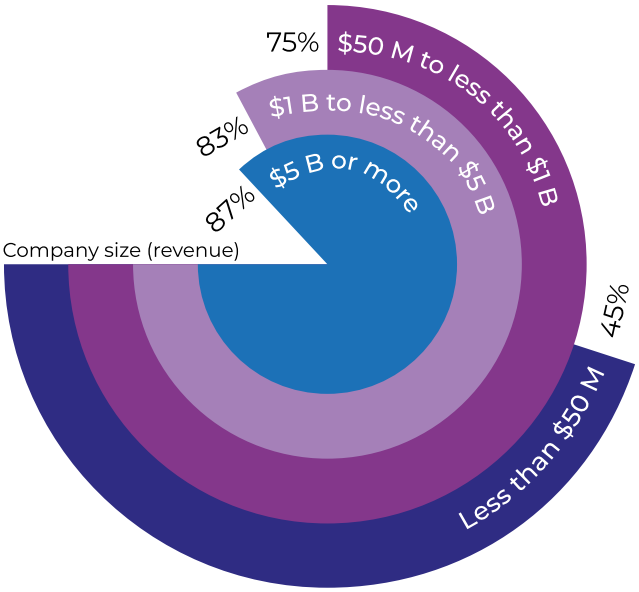
To the following question: *"How do the directors of your organisation monitor and keep updated on emerging risks?"*, Risk Managers were cited as the principal person that monitors and informs on emerging risks for 65% of Directors and Officers in the WTW survey covering 2023-2024.

It is also important for companies to set up programmes to train and raise employee awareness of their privacy and security obligations, and on how to detect and report any threats to the security of personal data or IT security systems.

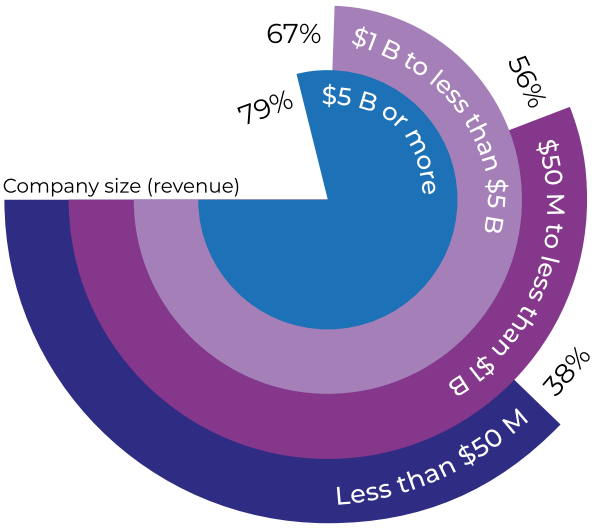


Note: 7% for 'Other'. Don't know was excluded.
Source: 2023/2024 WTW Directors & Officers Liability Insurance Survey.

Completed a cyber table-top exercise in the last 12 months



Feel that the organisation is well/very prepared to manage a cyber incident effectively



Source: 2023/2024 WTW Directors & Officers Liability Insurance Survey

Be prepared!

Preparation involves having at hand an incident response plan, ensuring effective communication within the organisation, and providing training.
It is also important to regularly assess and quantify cyber risks.
Completing a cyber table-top exercise is an effective way to be prepared for an event.
However, this exercise is often carried out differently by Small and Mid-Sized Enterprises, 45% of which have carried out such an exercise in the past 12 months, compared with big Corporates, a large majority of which – 87% - have carried out such an exercise in the last year.
Companies that have conducted a table-top exercise in the last 12 months feel that their organisation is well or very well prepared to manage a cyber incident effectively.

3/ Insurance considerations

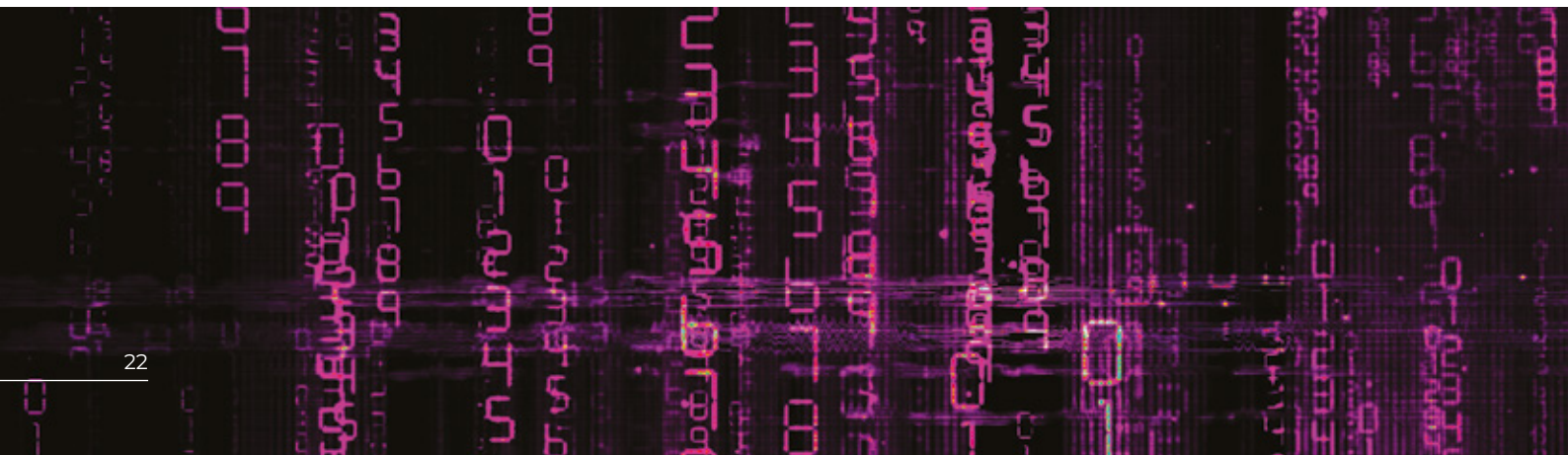
Transferring residual cyber risks to the insurance market also falls under the responsibilities of Risk and Insurance Managers.
Cyber insurance forms part of a comprehensive cyber risk management plan. It can help businesses reduce the financial impact of a cyber attack and provide expertise to respond to cyber incidents.
After three years of hard market conditions, cyber rates began to stabilise in 2023 and the first quarter of 2024 followed that trend.
Alternative risk transfer strategies can also be explored by Risk Managers either to provide an answer to non-insurable risks or to complete cyber insurance strategies.
Recently, Insured-Linked Securities (ILS) and Parametric policies have been added to the range of instruments available to Risk Managers for transferring risk.

CHAPTER 4

Policy recommendations

Based on this first-of-its-kind exercise aimed at linking the EU policy landscape to risk and insurance management, FERMA puts forward the following recommendations to European policymakers.

Issue	Recommendations
STRATEGIC UPDATE: The EU Cybersecurity Strategy was launched in 2020 and, despite progress, some key areas will need an update, not least addressing the reporting stack (below)	▪ FERMA supports the call from the Council of the EU under the Belgian Presidency on the European Commission to assess the results and gaps of the current EU Cybersecurity Strategy and its impact, and to present a revised strategy .
REPORTING STACK: Several requirements exist for cyber incident reporting and personal data breaches. This leads to possible overlaps and duplication in reporting obligations.	▪ European Commission, ENISA and other key stakeholders (such as Member States) to map cyber incident reporting requirements, ransomware reporting requirements, plus other cyber-related reporting requirements in order to identify the areas that could be simplified. ▪ Aim to reduce or simplify reporting requirements in line with European Commission's 25% target.
CASCADING COMMUNICATION COMPLEXITY: Just for the four EU legislations considered in this paper; there are four different possible recipients of incident reporting data: CSIRT, DPA, other national competent authority, and ENISA. At national level, there may be even more recipients (e.g. police or Regional government/authority).	▪ The European Commission to evaluate the concept of a "single point of entry" for cyber incident notification, as well as giving EU Member States some guidance on how to streamline the various entities involved.
ROLE OF THE RISK MANAGER: On one hand, the Risk Manager is ideally placed to oversee cyber risk governance and the treatment of cyber risks. On the other hand, in regulation there is not a consistent specification of what risk management measures enterprises must take, nor consideration of insurance implications.	▪ ENISA and the European Cybersecurity Competence Centre to stimulate cyber risk management best practices, especially for the SME segment. ▪ European Commission to consider the insurance/risk transfer implications of future EU cyber legislation.



1. EU regulations versus directives

The European Union is a political and economic union between its Member States and is made up of treaties. Treaties define the EU's objectives and the tools available to achieve them.
These tools include the types of legal acts that the EU can adopt, such as regulations and directives[6].
In recent years, cyber incident reporting obligations have been created and regulated by directives or regulations.
The choice of legislative instrument depends on whether the aim is to achieve objectives and leave member states some room for manoeuvre, or to be more prescriptive and detailed. The reason for this choice may also be expressed within the legal act itself (most of the time in the recitals).
For example, if the scheme is too detailed and no longer leaves room for discretion, the appropriate instrument will be a regulation rather than a directive, the main difference between these two instruments being the transposition or direct application (A).

A/ TRANSPOSITION VS. DIRECT APPLICATION

"(...) A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods (...)."[7]
Directives are legislative acts that set targets for EU countries, it is binding on the Member States to which it is addressed (one, several or all) as regards to the result to be achieved while leaving the national authorities' discretion as to the form and means of achieving it.

Directives are adopted by the European institutions based on treaties.
Once adopted at EU level, they are then transposed by the EU Member States to become law in the Member States.
It is up to each Member State to develop its own legislation to determine how the rules laid down by the directive are to be applied.
Therefore, a directive is not directly applicable in Member States, it must first transpose it into national law. Transposition is mandatory and must take place by the deadline set in the directive.
If a Member State does not comply with this obligation, the European Commission may initiate infringement proceedings and bring the case before the Court of Justice of the European Union (CJEU). Failure to comply with the ruling of the CJEU may result in a conviction which may lead to a fine.
National authorities are required to notify the European Commission of national measures aimed at achieving the objectives of the directive. Where a Member State fails to do so, the Commission may impose a fine on the Member State in question[8].
A directive only takes effect once it has been transposed. However, the CJEU considers that a directive that is not transposed can have certain direct effects when the transposition into national law has not taken place or has been carried out incorrectly and/or the terms of the directive confer right on individuals.
Where these conditions are met, individuals may invoke the directive against a Member State ("vertical direct effect") before the national courts but not against another individual ("horizontal direct effect")[9].

A transposition scoreboard is updated every year as part of the Single Market Scoreboard and is available for all the Member States of the EU and also per country. At the time of writing this white paper, it is available here: https://single-market-scoreboard.ec.europa.eu/ https://single-market-scoreboard.ec.europa.eu/enforcement-tools/transposition_en Details of the transposition of specific legislation by country are available on the EUR-LEX website.

The directive can set minimum or maximum (full) harmonisation requirements. The standards of harmonisation are lower, often when the EU recognises that the legal systems in some Member States already have higher standards. In this case, Member States have the right to establish higher standards than those define in the directive.

"(...) A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States (...)."[10]
Regulations are also adopted by EU institutions based on treaties. They aim to ensure uniform application of EU legislation in all EU countries.
A regulation must be fully complied with by those to whom it applies.
A regulation applies directly in the Member States after the date of entry into application specified in the text, without having to be transposed into national law. From this date, a regulation can be invoke directly before national courts and can be used as a reference between individuals or with other individuals, Member States and EU authorities.
It is also important to understand the difference between the entry into force of a legal act and its transposition date or application date (B).

B/ IN FORCE VS. TRANSPOSITION/APPLICATION DATE

A regulation or a directive enters into force on the date specified in the act (in general, in the latest articles), or, where applicable, 20 days after its publication in the Official Journal of the European Union (OJEU).
The application date may be different from the date the regulation, or the directive enters into force.
A directive will leave a transposition period for the Member States, at the end of which the measures necessary to comply with the directive must be applied.
A regulation may also provide for a period of adaptation to its measures before being directly applicable in the Member States.
For example, the directive Network and Information Security (NIS) which entered into force on the 20th day following its publication in the OJEU on 19 July 2016, i.e. 8 August 2016, had to be transposed by 9 May 2018 for the national measures to be applied by 10 May 2018.
The GDPR entered into force on the 20th day following its publication in the OJEU on 4 May 2016, i.e. 24 May 2016, but came into application on 25 May 2018.
See table at the end of Chapter 1.
Let's now go into more details about the regulations, the ones in force and application (2) and the forthcoming ones (3) which impose an obligation to notify in the event of a cyber incident.

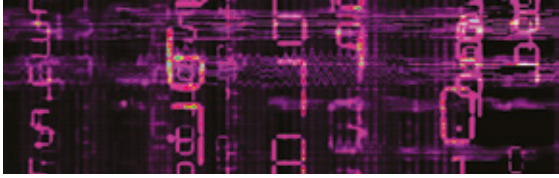
2. Detailed categorisation of EU rules

For each regulation, we will determine its type, the application date, the notification and communication requirements (for what and to whom, the deadline, the content) and the sanction applicable in the event of non-compliance.
Currently in force and in application are the GDPR (A) and the NIS1 Directive (B).

A/ GDPR

The GDPR protects individuals when their data is being processed by the private sector and most of the public sector.
All companies worldwide that process personal data of EU citizens must comply with this regulation.

- Type: regulation, binding in its entirety and directly applicable in all Member States.
- Key date: applicable since 25 May 2018 (article 99(2)).
- Sectors and entities: GDPR applies to all companies either public (the processing of data by the relevant authorities for law enforcement purposes is regulated by the data protection law enforcement directive) either private, worldwide that process personal data of EU citizens.
- Notification and Communication requirements:
  • For what and to whom?
  Companies and organisations [the data controller] must notify the relevant data



protection supervisory authority in case of a personal data breach unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (article 33(1)).
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate the personal data breach to the data subject (article 34(1)).
The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with article 33 (article 33(5)).
In case of cross-border processing (article 4(23)), the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority (article 55(1)).

• **Deadline:**

The data protection supervisory authority shall be notified without undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach.
Where the notification to the data protection supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay (article 33(1)).
For the communication to the data subjects: without undue delay (article 34(1)).

• **Content:**

The notification to the data protection supervisory authority shall at least (article 33(3)):
"(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."
As for the communication to the data subjects, it shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of article 33(3)) (article 34(2)).
Article 34(3) provides for cases where the communication to the data subject shall not be required: "(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b)the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c)it would involve disproportionate effort.
In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner."

Sanction

Article 82(1) provides that "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."
Failure to comply with articles 33 and 34 can lead to "(...) administrative fines up to €10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (...)" (article 83(4)).
Article 83(6) provides that "Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to €20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."

B/ NIS1

The NIS1 directive sets measures to achieve a high common level of security of network and information systems to secure vital services to the EU.

- Type: directive that had to be incorporated into national law.

- Key date: measures necessary to comply with NIS1 had to be adopted by the Member States and have been applicable since 10 May 2018 (article 25(1)).

- Sectors and entities:
  Article 5(1) states that for each sector and subsector referred to in Annex II
  1. Energy: Electricity, Oil, Gas
  2. Transport: by Air, Rail, Water, Road
  3. Banking
  4. Financial market infrastructures
  5. Health sector: health care settings (including hospitals and private clinics)
  6. Drinking water supply and distribution
  7. Digital Infrastructure
  Member States shall identify Operators of Essential Services (OES) with an establishment on their territory.
  The criteria for the identification of the OES are as follows according to article 5(2):
  • "(...) (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
  • (b) the provision of that service depends on network and information systems;
  • and (c) an incident would have significant disruptive effects on the provision of that service."
  The NIS1 directive also applies to Digital Service Providers (DSP) providing the following services: online marketplace, online search engine and cloud computing service (annex III) (article 1(1d)) even if it is not established in the E.U (article 18(2))

- Notification requirements:
  • For what and to whom?
  OES (article 14(3)) must notify, the competent authority or the Cyber Security Incident Response Team (CSIRT) of incidents having a significant impact on the continuity of the essential services they provide.
  To determine the "significance" of the impact of an incident (article 14(4)), the specific following parameters shall be taken into account:
  • "(a) the number of users affected by the disruption of the essential service;
  • (b) the duration of the incident;
  • (c) the geographical spread with regard to the area affected by the incident."
  DSP (article 16(3)) must notify, the competent authority or the CSIRT of any incident having a substantial impact on the provision of a service (as referred to in Annex III) that they offer within the Union.
  To determine whether the impact of an incident is "substantial" (article 16(4)), the following parameters in particular shall be taken into account:
  • "(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services;
  • (b) the duration of the incident;
  • (c) the geographical spread with regard to the area affected by the incident;
  • (d) the extent of the disruption of the functioning of the service;
  • (e) the extent of the impact on economic and societal activities."
  The mandatory notification shall only apply where the DSP has access to the information needed to assess the impact of an incident against the parameters mentioned above.
  Article 16(5) provides that where an OES relies on a third-party DSP for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the DSP shall be notified by that operator.
  Moreover, article 16(7) states that after consulting the DSP concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the DSP to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.

- **Deadline:** without undue delay (article 14(3)).
- **Content:** notification shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident (article 14(3)).

- Sanction:
  Article 21 states that "Member States shall lay down the rules on penalties applicable to any infringement of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for, shall be effective, proportionate and dissuasive. (...)"
  An assessment of the approach adopted by Member States in implementing the NIS1 Directive revealed a lack of consistency between Member States and a low level of common response in the event of a crisis. The NIS directive will be repealed by the NIS2 directive which addresses its weaknesses. NIS2, which is already in force but not yet applicable, reinforces the obligation to notify, and is part of an expanding legislative environment since two other European regulations have been adopted in the wake of it, also providing for an obligation to notify.

3/ Focus on key forthcoming EU regulations on notification requirements

A/ NIS2

NIS2 sets out a high common level of cybersecurity across the EU, introducing cybersecurity risk-management measures and reinforcing reporting in critical sectors.

- Type: Directive that must be incorporated into national law.

- Key date: Measures necessary to comply with NIS2 to be adopted by the Member States and applied from 18 October 2024 (article 41(1)).

- Sectors and entities:
  The directive applies mainly to medium-sized and large public or private entities operating in sectors as defined in Annex I (sectors of high criticality) or II (other critical sectors) which provide their services or carry out their activities within the Union (article 2(1)).
  Exceptions to the size criteria are mentioned in article 2(2)(3)(4).

Annex I – sectors of high criticality

- **Energy:** electricity, including production, distribution and transmission systems and charging points; district heating and cooling; oil, including production, storage and transmission pipelines; gas, including supply, distribution and transmission systems and storage; and hydrogen.
- **Transport** by air, rail, water and road.
- **Banking and financial market infrastructures** such as credit institutions, operators of trading venues and central counterparties.
- **Health,** including healthcare providers, manufacturers of basic pharmaceutical products and critical medical devices, and EU reference laboratories.
- **Drinking water.**
- **Waste water.**
- **Digital infrastructure,** including providers of data centre services, cloud computing services, public electronic communications networks and publicly available electronic communications services.
- **ICT managed services** (business-to-business).
- **Space.**
- **Public administration** at the central and regional level, excluding judiciary, parliaments, and central banks.
  However, it does not apply to public administration entities that carry out activities in the areas of national security, public security, defence or law enforcement.

Annex II – other critical sectors

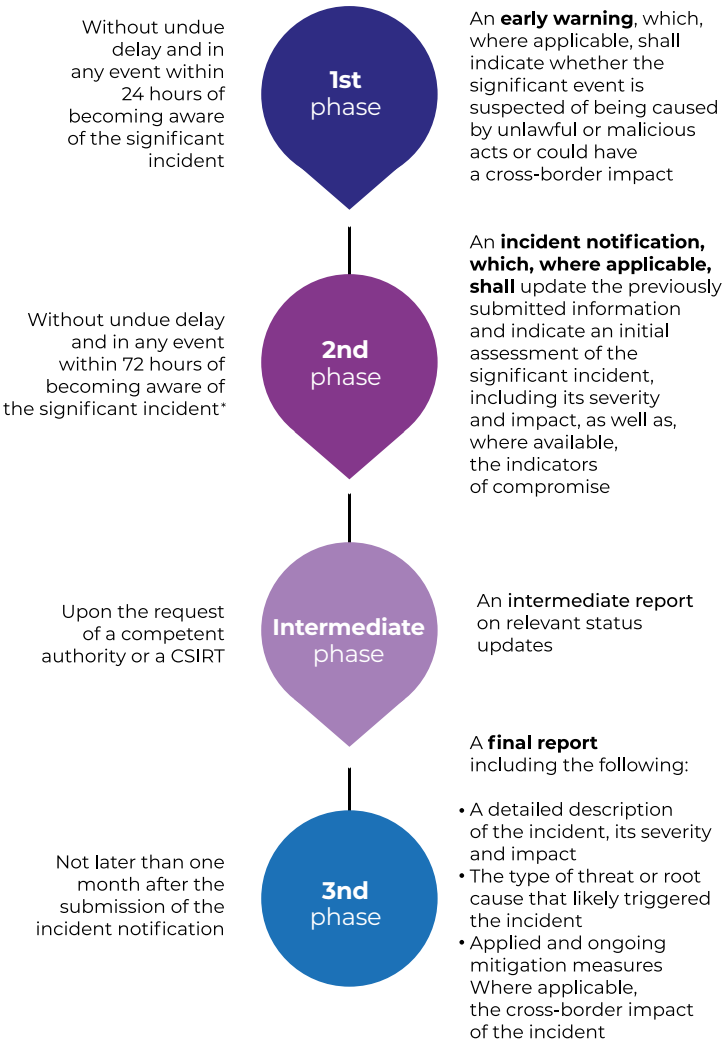
- **Postal and courier services;**
- **Waste management;**
- **Chemical** manufacturing, production and distribution.
- Food production, processing and distribution.
- **Manufacturing,** specifically medical devices, computer, electronic and optical products, certain electrical equipment and machinery, motor vehicles and other transport equipment.
- **Digital providers** of online marketplaces, search engines and social networks; and
- **Research organisations**

NIS2 defines two type of entities (article 3): “essential entities” and “important entities”. There are 7 types of essential entities. Essential entities are mainly of a type referred to in Annex I and of a large size (article 3(1)(a)). NIS2 contains a few exceptions to the size threshold (including medium-sized enterprises). Entities that were identified as OES within the NIS1 before 2023, January 16th are also qualified as essential entities (article 3(1)(g)).
Entities of a type referred to in Annex I or II that do not fall within the definition of essential entities are considered as important entities by default (article 3(2)).

- Notification and Communication requirements:

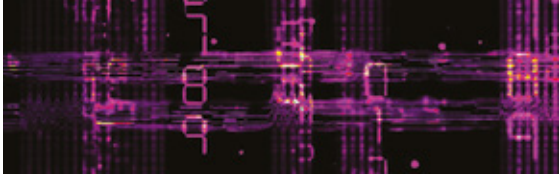
  • For what and to whom?

  Notification can be twofold:
  First, entities must notify their CSIRT or relevant authority of any incident that has a significant impact on the provision of their services (article 23(1)).
  And where appropriate, entities concerned shall notify, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. A significant incident is an incident that (article 23(3)):
  - has caused or is capable of causing severe operational disruption or financial loss for the entity;
  - has affected or could affect others by causing considerable material or non-material damage.
  A communication must be made, where applicable, to the recipients of the entities’ services that are potentially affected by a significant cyber threat on any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself (article 23(2)).
  A “significant cyber threat” is defined by article 6(11) as “a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity’s services by causing considerable material or non-material damage”.
  • **Timeline/ deadline and content:** this is one of the new features introduced by NIS2. Article 23(4) sets out reporting obligations in three phases:



In the event of an ongoing incident at the time of the submission of the final report, Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

*By way of derogation a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.



- Sanction

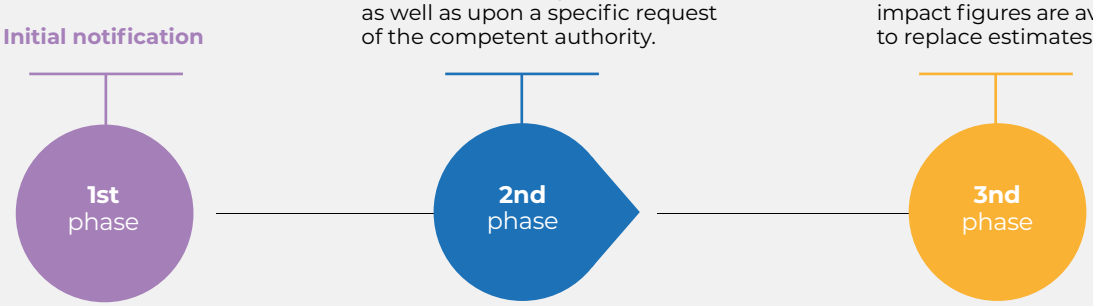
The directive provides for supervisory and enforcement measures, including the possibility for authorities to order the entities concerned to inform the natural or legal persons including any possible protective or remedial measures which can be taken by them in response to that threat (article 32(4(e)) for essential entities and article 33(4(e)) for important entities).
Article 32(6) provides that it is possible to hold any natural person responsible for breach of their duties to ensure compliance with this directive.
Article 32(7) provides that when it comes to taking enforcement measures in relation to essential entities, the competent authorities shall, as a minimum, take due account of, in particular the seriousness of the infringement and the importance of the provisions breached. Failure to notify significant events constitutes a serious infringement (article 32(7(ii)). The same applies for important entities (article 34(5)).
In addition to enforcement measures, effective, proportionate and dissuasive administrative fines shall be imposed in respect of infringements (article 34(1)(2)).
Pursuant to article 34(3): when deciding whether to impose an administrative fine and deciding on its amount in each individual case, due regard shall be given, as a minimum, to the elements provided for in article 32(7).
We emphasise that this article cites the failure to notify as a serious breach.
Essential entities that infringe their reporting obligations (article 34(4)) are subject to administrative fines of a maximum of at least €10 million of a maximum of at least 2% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.
Important entities that infringe their reporting obligations (article 34(5)) are subject to administrative fines of a maximum of at least €7 million or of a maximum of at least 1,4% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.

With regards to sanction, this directive is quite similar to the GDPR, and this is a big change compared to the NIS1.
Let's now take a look at the Digital Operational Resilience Act (DORA) regulation, which applies to the financial sector. DORA constitutes lex specialis with regard to NIS2 for the financial sector (recital 16 of the DORA). For entities affected by DORA, this text therefore takes precedence over NIS2. However, this does not mean that NIS2 obligations are cancelled for entities affected by both texts. DORA complements rather than overrides NIS2 and addresses possible overlaps with the lex specialis exemption.

DORA further harmonizes the requirements set out in the NIS2 directive for financial entities and their ICT service providers. Nevertheless, the importance of maintaining a close link between the financial sector and the Union's horizontal cybersecurity framework as currently defined in the NIS2 Directive has been identified, in order to ensure consistency with the cybersecurity strategies adopted by the Member States and to enable financial supervisors to be informed of cyber incidents affecting other sectors covered by the said directive to enable cross-sector learning and to effectively draw on experiences of other sectors in dealing with cyber threats (recital 18 of the DORA).

B/ DORA

This regulation which specifically applies to financial undertakings and ICT third-party service providers defines uniform requirements to strengthen and harmonize risk management for information and communication technologies (ICT) and the security of networks and information systems at EU level.
DORA creates a regulatory framework for digital operational resilience, enabling financial entities to ensure that they can withstand, respond to and recover from any serious operational disruption related to ICT.
Among the 5 essential pillars identified by the DORA regulation that financial institutions

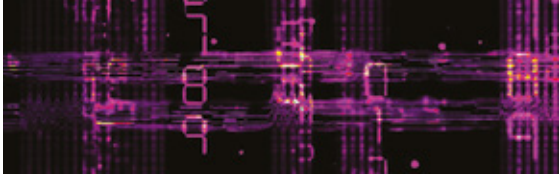


must put in place is incident management, with harmonized, centralized reporting to competent authorities.
Digital operational resilience as defined by DORA means "the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions;" (article 3(1)).

- Type: regulation, binding in its entirety and directly applicable in all Member States.
  Alongside the DORA regulation, an associated Directive will amend existing directives to align them with the provisions of the regulation.
  For example, credit institutions that must report incidents under the DORA previously had to report under the PSD2 Directive (recital 7 of the new Directive).

- Key date: applicable from 17 January 2025 (article 64). The directive must be transposed by Member States by 17 January 2025 (article 9).

- Sectors & Entities: article 2(1)
  - **"financial entities" (20 types):**
  (a) credit institutions;
  (b) payment institutions
  (c) account information service providers;
  (d) electronic money institutions
  (e) investment firms;
  (f) crypto-asset service providers and issuers of asset-referenced tokens;
  (g) central securities depositories;
  (h) central counterparties;
  (i) trading venues;
  (j) trade repositories;
  (k) managers of alternative investment funds;
  (l) management companies;
  (m) data reporting service providers;
  (n) insurance and reinsurance undertakings;
  (o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;
  (p) institutions for occupational retirement provision;
  (q) credit rating agencies.
  (r) administrators of critical benchmarks;
  (s) crowdfunding service providers.
  (t) securitisation repositories;
  (u) ICT third-party service providers



Communication, Notification and Information requirements

• For what and to whom?

DORA requires a number of preventive actions to be taken. Article 14 provides that, as part of the ICT risk management framework, financial entities shall:

- have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.
- implement communication policies for internal staff and for external stakeholders.

Article 17(1) provides that financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.
Article 18 provides that financial entities shall classify ICT-related incidents and shall determine their impact on certain criteria (number and/or relevance of clients, duration of the incident, geographical spread, data losses entailed, criticality of the service affected, the economic impact).
Article 19(1) states that financial entities shall report major ICT-related incidents to the relevant competent authority.
Where a financial entity is subject to supervision by more than one national competent authority, Member States shall designate a single competent authority as the relevant competent authority responsible for carrying out the functions and duties provided for in this article.
Article 3(10) 'major ICT-related incident' means "an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the financial entity;"
An initial notification and reports shall be produced using the templates referred to in article 20 of the Regulation. If a technical impossibility prevents the submission of the initial notification using the template, financial entities shall notify the competent authority about it via alternative means (article 19(1)).

• Deadline and Content (article 19(4))

Without prejudice to the reporting by the financial entity to the relevant competent authority, Member States may additionally determine that some or all financial entities shall also provide the initial notification and each report using the templates to the competent authorities or the computer security incident response teams (CSIRTs) designated or established in accordance with the NIS2 Directive (article 19(1)).
Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients.

Article 19(3) provides that where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident.
In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.
Article 19(5) states that financial entities may outsource the reporting obligations under this article to a third-party service provider.
In case of such outsourcing, the financial entity remains fully responsible for the fulfilment of the incident reporting requirements.
Credit institutions, payment institutions, account information service providers, and electronic money institutions must report major operational or security payment-related incidents to the competent authorities (articles 1(1(a)(iii) and 23).
Article 3(11) 'major operational or security payment-related incident' means an operational or security payment-related incident that has a high adverse impact on the payment-related services provided;

- Sanctions:
  article 50(3): without prejudice to the right of Member States to impose criminal penalties, Member States shall lay down rules establishing appropriate administrative penalties and remedial measures for breaches of this Regulation and shall ensure their effective implementation. Those penalties and measures shall be effective, proportionate and dissuasive.

Member States shall confer on competent authorities the power to apply at least the following administrative penalties or remedial measures for breaches of this Regulation (article 50(4)):
(a) issue an order requiring the natural or legal person to cease conduct that is in breach of this Regulation and to desist from a repetition of that conduct;
b) require the temporary or permanent cessation of any practice or conduct that the competent authority considers to be contrary to the provisions of this Regulation and prevent repetition of that practice or conduct;
c) adopt any type of measure, including of pecuniary nature, to ensure that financial entities continue to comply with legal requirements;
(d) require, insofar as permitted by national law, existing data traffic records held by a telecommunication operator, where there is a reasonable suspicion of a breach of this Regulation and where such records may be relevant to an investigation into breaches of this Regulation; and
(e) issue public notices, including public statements indicating the identity of the natural or legal person and the nature of the breach.
To a certain extent, administrative penalties and remedial measures, subject to the conditions provided for in national law, shall be applied to members of the management body, and to other individuals who under national law are responsible for the breach (article 50(5)).
The web of cybersecurity protection continues to be woven by the EU that is, in the course of adopting a new regulation in the area of products with digital elements this time. Let's now examine the future Cyber Resilience Act (CRA) that will complement the NIS2 framework.

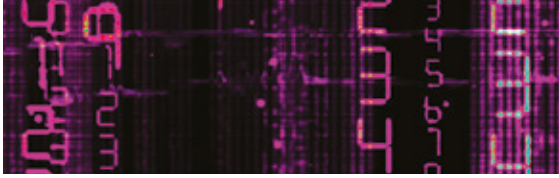
C/ CRA

The CRA will introduce common cybersecurity rules for products available on the EU with digital elements throughout their life cycle and ancillary services. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. The European Parliament adopted the Act on 12 March 2024. The next step is adoption by the Council, followed by publication in the OJEU. The CRA will enter into force on the 20th day following its publication in the OJEU. It will then come into application from 36 months after the date of entry into force. However, article 14, which concerns us, shall apply from 21 months after the date of entry into force of this Regulation. This white paper is based on the text approved by the European Parliament.

- Type: proposal for a Regulation which shall be binding in its entirety and directly applicable in all Member States.

- Key date: expected to apply by 2027 except the reporting obligations expected to apply by 2026 (article 71(2)).

- Sectors & Entities: the CRA applies to "economic operators": manufacturers (or their authorised representative) who develop or manufacture "products with digital elements" or has products with digital elements designed, developed, or manufactured, and market them under their name or trademark, whether for payment, monetisation or free of charge (article 3(13)) as well as to importers and distributors of such products.
  The CRA applies to entities inside and outside the EU insofar as these entities make available on the EU market products in scope of the Regulation.
  The products concerned are products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network (article 2(1)).
  A product with digital elements under the CRA is any software or hardware product and its remote data processing solutions, including



software or hardware components being placed on the market separately (article 3(1)). The regulation excludes from its application certain products with digital elements, for example, those which are already regulated by Union legal acts such as medical devices (article 2(2)(a)) or in vitro diagnostic medical devices (article 2(2)(b)).

- Relationship with NIS2 and other sectorial Union legal acts: Directive NIS2 does not directly cover mandatory requirements for the security of products with digital elements (recital 3 of the CRA). The CRA, by enhancing the level of cybersecurity of products with digital elements, will ease compliance by entities in scope of the NIS2 directive (recital 24 of the CRA). As the CRA only covers products with digital elements sold within the EU market, software provided as part of a service will not be covered by the CRA (recital 12). Technical requirements for cybersecurity of systems provided as a service or developed in-house are regulated by the NIS2 directive or other specific Union legal acts with the same level of protection.

- Notification and Information requirements:

  • For what and to whom?

  Requirements on manufacturers are the following: First, a manufacturer is requested to notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA (article 14(1)).
  "Actively exploited vulnerability" is defined under the CRA (article 3(42)) as "a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without permission of the system owner".
  A "vulnerability" is "a weakness, susceptibility or flaw of a product with digital elements that can be exploited by a cyber threat" (article 3(40)).
  The obligations laid down in article 14(1) shall apply to open-source software stewards (defined at article 3(14)) to the extent that they are involved in the development of the products with digital elements (article 24(3)).

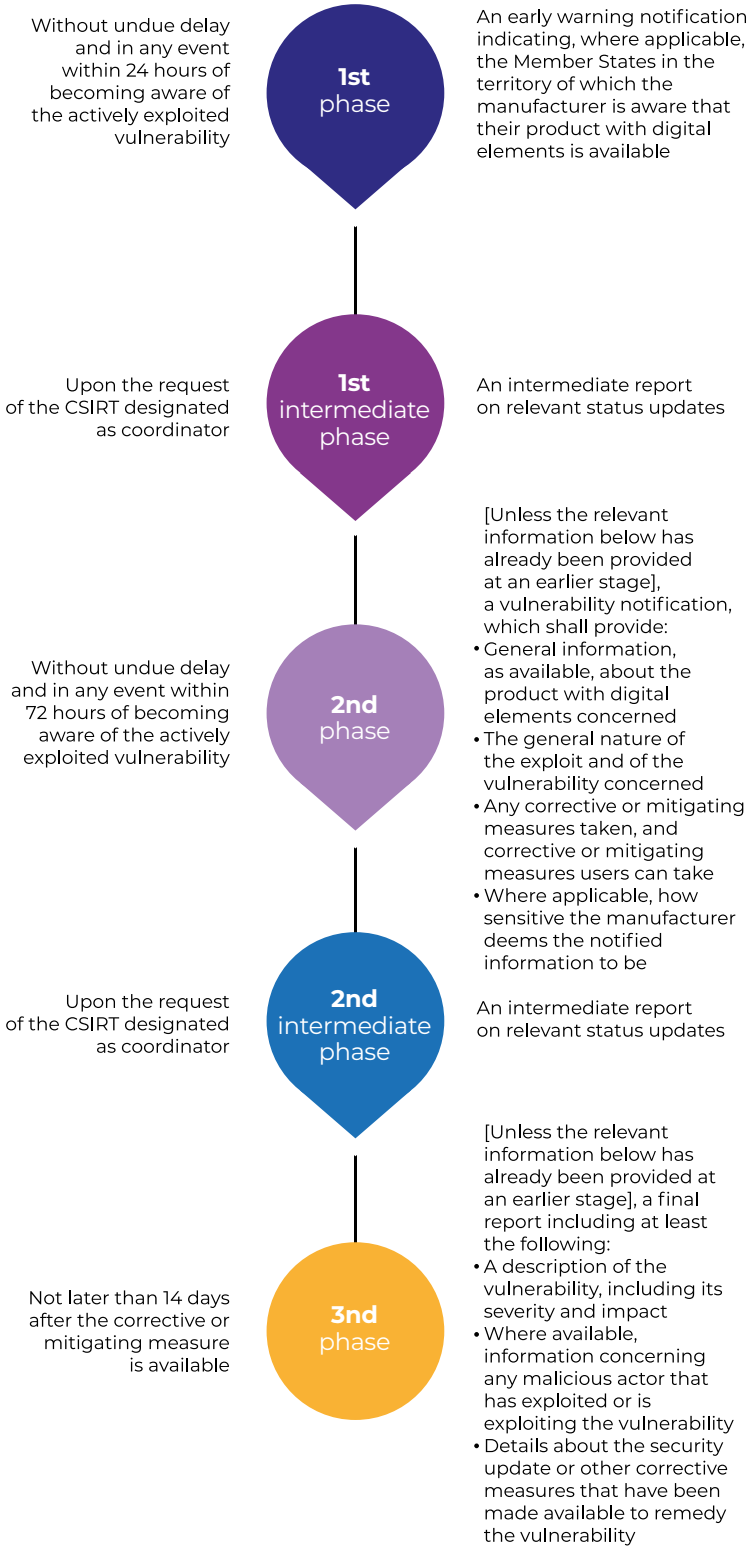
Secondly, a manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator and to ENISA (article 14(3)).

"Incident having an impact on the security of the product with digital elements" is defined under the CRA (article 3(44)) as an "incident that negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of data or functions".

An incident having an impact on the security of the product with digital elements shall be considered to be severe, where (article 14(5)):
"(a) it negatively affects or is capable of negatively affecting the ability of a product with digital elements to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions; or
(b) it has led or is capable of leading to the introduction or execution of malicious code in a product with digital elements or in the network and information systems of a user of the product with digital elements."

Thirdly, manufacturers also have the obligation to inform after becoming aware of an actively exploited vulnerability or a severe incident, the impacted users of the product with digital elements, and where appropriate all users, about the actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements and, where necessary, about risk mitigation and any corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident (article 14(8)).

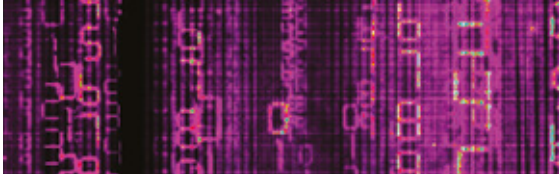
The obligations laid down in article 14(3) and (8) shall apply to open-source software stewards to the extent that severe incidents having an impact on the security of products with digital elements affect network and information systems provided by the open-source software stewards for the development of such products (article 24(3)).

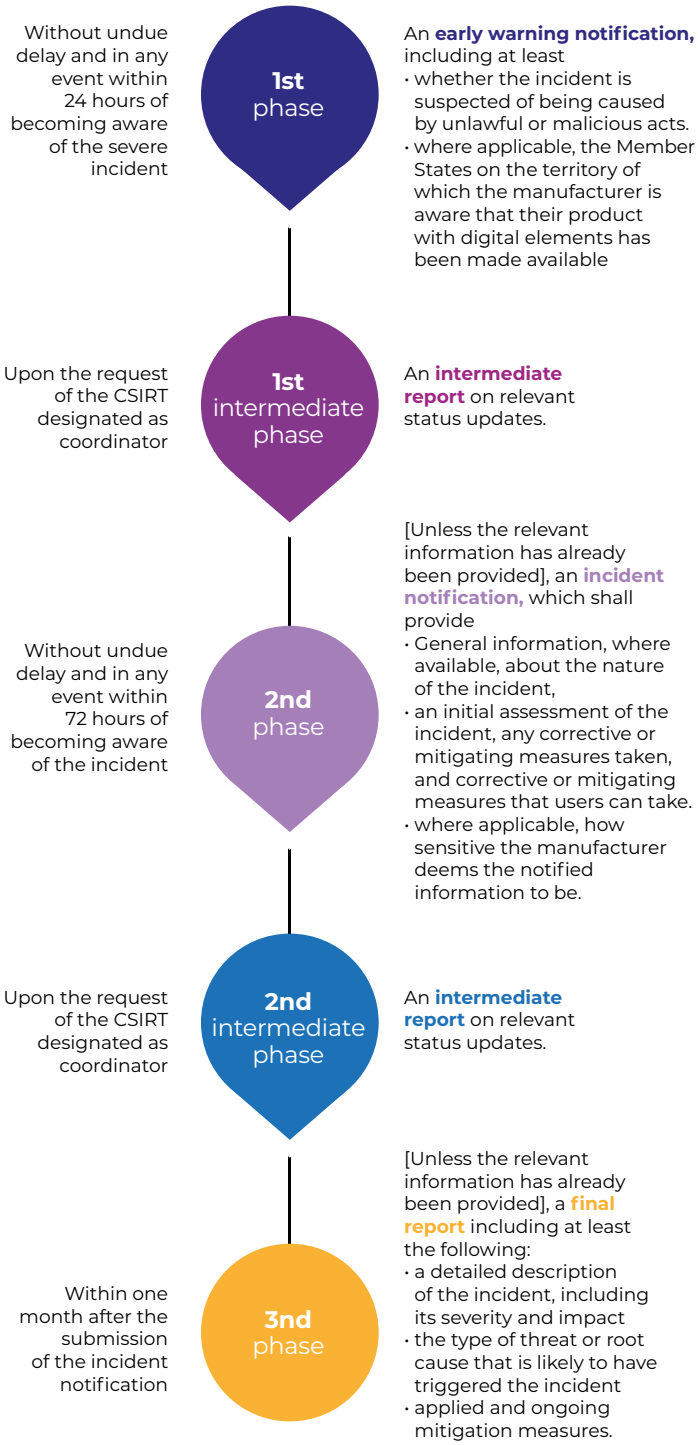


The CRA sets out cases in which manufacturers' obligations apply to importers and distributors (article 21) and to a natural or legal person other than the manufacturer, the importer or the distributor (article 22) for the purposes of this Regulation.
This includes the reporting obligations from article 14.
"An importer or distributor shall be considered a manufacturer (...) where that importer or distributor places a product with digital elements on the market under its name or trademark or carries out a substantial modification of the product with digital elements already placed on the market" (article 21).
"A natural or legal person, other than the manufacturer, the importer or the distributor, that carries out a substantial modification of the product with digital elements and makes it available on the market, shall be considered a manufacturer. That person shall be subject to [reporting obligations] for the part of the product with digital elements that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product" (article 22).

• Timeline/ Deadline/ Content
Notification obligations under the CRA operate in phases, as in the NIS2 directive.
Notification phases for actively exploited vulnerabilities

The manufacturer shall notify any actively exploited vulnerability via the single reporting platform to be established by the CRA using the electronic notification endpoints of the CSIRT designated as coordinator of the Member State where the manufacturer has its main establishment and shall be simultaneously accessible to ENISA.





Notification phases for severe incidents having an impact on the security of the product with digital elements.

A manufacturer shall be considered to have its main establishment within the Union, in the Member State where the decisions related to the cybersecurity of its products with digital elements are predominantly taken.

For the “CSIRT designated as coordinator”, the CRA (article3(51)) refers to article 12(1) of the NIS2 directive, which provides that each member state must designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure.
The CSIRT designated as coordinator shall act as a trusted intermediary, facilitating, where necessary, the interaction between the natural or legal person reporting a vulnerability and the manufacturer or provider of the potentially vulnerable ICT products or ICT services, upon the request of either party.
The tasks of the CSIRT designated as coordinator shall include: identifying and contacting the entities concerned; assisting the natural or legal persons reporting a vulnerability; and negotiating disclosure timelines and managing vulnerabilities that affect multiple entities.

Where a reported vulnerability could have a significant impact on entities in more than one Member State, the CSIRT designated as coordinator of each Member State concerned shall, where appropriate, cooperate with other CSIRTs designated as coordinators within the CSIRTs network.
The information from manufacturers to users shall be, where appropriate, in structured and easily
automatically processible machine-readable format. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRT may provide such information to the users when considered proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident (article 14(8)).
The CSIRTs designated as coordinators shall provide helpdesk support in relation to the reporting obligations to manufacturers and in particular manufacturers that qualify as microenterprises or as small or medium-sized enterprises (article 17(6)).
It is important to note that the European Commission in cooperation with the CSIRTs network and ENISA may further specify the format and procedures of the notifications through implementing acts (article 14(10)).

A voluntary reporting scheme is provided for at article 15 for:

- any vulnerability contained in the product with digital elements,
- cyber threats that could affect the risk profile of such products
- any incident having an impact on the security of such products
- near misses that could have resulted in an incident having an impact on the security of the product with digital elements

- Sanction:

  Member States shall lay down the rules on penalties applicable to infringements of the CRA and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive (article 64).

  The non-compliance with the obligations set out in, in particular, article 14 shall be subject to administrative fines of up to €15 millionor, if the offender is an undertaking, up to 2.5% of its total worldwide annual turnover for the preceding financial year, whichever is higher (article 64(2)).

  The non-compliance with the obligations set out in, in particular, in articles 18 to 23 shall be subject to administrative fines of up to €10 millionor, if the offender is an undertaking, up to 2% of its worldwide annual turnover for the preceding financial year, whichever is higher (article 64(3)).

  When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

"(a) the nature, gravity and duration of the infringement and of its consequences;
(b) whether administrative fines have been already applied by the same or other market surveillance authorities to the same economic operator for a similar infringement;
(c) the size, in particular with regard to microenterprises, small and medium sized enterprises, including start-ups, and the market share of the economic operator committing the infringement" (article 64(5)).

Market surveillance authorities that apply administrative fines shall communicate that application to the market surveillance authorities of other Member States (article 64(6)).
Each Member State shall lay down rules on whether and to what extent administrative fines may be imposed on public authorities and public bodies established in that Member State (article 64(7)).
Administrative fines may be imposed, depending on the circumstances of each individual case, in addition to any other corrective or restrictive measures applied by the market surveillance authorities for the same infringement (article 64(9)).

By way of derogation, according to article 64(10), administrative fines shall not apply to the following:
a) manufacturers that qualify as microenterprises or as small enterprises with regard to any failure to meet the deadlines for the early warning notifications on an actively exploited vulnerability or severe incident;
b) any infringement of this Regulation by open-source software stewards.

NOTES:

NOTES:

About FERMA

The Federation of European Risk Management Associations brings together 23 national risk management associations from 22 European countries. FERMA represents the interests of more than 5,500 risk and insurance managers in Europe active in a wide range of business sectors from major industrial and commercial companies to financial institutions and local government bodies. More information can be found at www.ferma.eu

About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organisational resilience, motivate your workforce and maximise performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

---

(1) Ransomware, Disclosure and Whistleblowing: The New Winning Combination for Cyber Criminals by Laure Zicry, Martin Twells, Dean Chapman, Jake Wingfield 18 September 2020, WTW
(2) (under article L.12-10-1)
(3) [pursuant to Articles 323-1 to 323-3-1 of the Criminal Code]
(4) "Article 2: Scope: 1. Without prejudice to paragraphs 3 and 4, this Regulation applies to the following entities: a) credit institutions,"
(5) Council of the EU, 'Council conclusions on the future of cybersecurity: implement and protect together', 21 May 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/cybersecurity-council-approves-conclusions-for-a-more-cyber-secure-and-resilient-union/
(6) Article 288 Treaty on the Functioning of the European Union (TFEU) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E288
(7) ibid.6
(8) Article 260 TFEU, para 3 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E260
(9) Vertical direct effect: Judgment in Case C-41/74 Yvonne van Duyn v Home Office; No horizontal direct effect: Judgment in Case C-152/84 M. H. Marshall v Southampton and South-West Hampshire Area Health Authority (Teaching).
(10) Ibid.6
(11) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
(12) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

FERMA

Anticipating changes
Shaping the future

with the support of

wtw