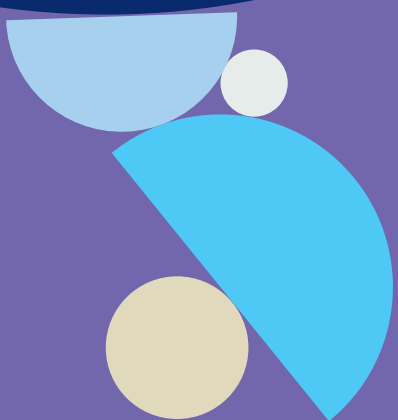
ZURICH

CYBER THREAT ALLIANCE

CyberGreen

Cyber metrics for key decision-makers



Contents

Section 1

Enhancing cyber security: Key metrics for policymakers

Cyber security is about keeping digital environments secure from risks so individuals and organizations can operate safely and confidently. It is a multifaceted issue that defies simple solutions. But one thing is certain: Without accurate, timely and comprehensive data, organizations are essentially *flying blind* in their cyber defenses.

Like other complex data-driven global challenges, using key metrics to guide decisions can lead to significant improvements. Much work has been dedicated to the corporate level. There are national and regional initiatives such as the European Union Agency for Cybersecurity (ENISA) or the U.S. Cybersecurity and Infrastructure Security Agency (CISA) which provide frameworks and resources to guide organizations in strengthening their cyber defenses.

However, national-level cyber security metrics that enable governments to make informed policy decisions remain largely absent. This paper introduces six key metrics and a supporting institutional framework to address this gap.

Collaboration on cyber data

Effective metrics at the national or aggregate level will create better framework conditions for the safety of all parts of the economy, helping to protect critical infrastructures as well as small and medium-sized enterprises (SMEs) that form the backbone of the economy. They should focus on general resilience, preparedness and response capabilities, adapted by industry, the threat landscape and the size of companies. These metrics would give policymakers the ability to assess relative strengths and weaknesses within existing regulatory frameworks, so that they can see what is working and where adaptations may be needed. To get there, public and private sector collaboration will be essential. Sharing data on what's happening *in the wild* and what subsequently materializes into cyber incidents affecting public infrastructure, organizations, defenses and responses, is a key enabler to develop comprehensive strategies against cyber threats.

Helping to bridge the cyber risk protection gap

The development of cyber metrics will also allow society to address the persistent cyber risk protection gap, a societal challenge that requires collective action and collaboration from both the insurance industry and the public sector (see Zurich's previous white paper on *Closing the Cyber Risk Protection Gap*). Despite the cyber insurance market's strong growth over recent years, this gap, reflecting the economic loss of a cyber event compared to the losses insured by the re/insurance industry, is estimated to have grown to a staggering USD 0.9 trillion, with insured losses only covering 1 percent of economic losses.

As outlined in the whitepaper, reducing the cyber risk protection gap requires strategies along three pillars (see illustration 1):

(1) Strengthening cyber resilience through such measures as raising awareness and education regarding cyber risks, providing subsidies for investment into cyber security, using cyber resilience services offered by the insurance industry, and sharing structured data.

(2) Addressing quantifiable catastrophic cyber risk, which in general is insurable, through traditional or alternative re/insurance markets. However, loss events above a significant threshold (e.g., a multiple of the cyber insurance market's overall global gross written premium volume) can have severe financial accumulation potential and will require solutions beyond the private cyber insurance market.

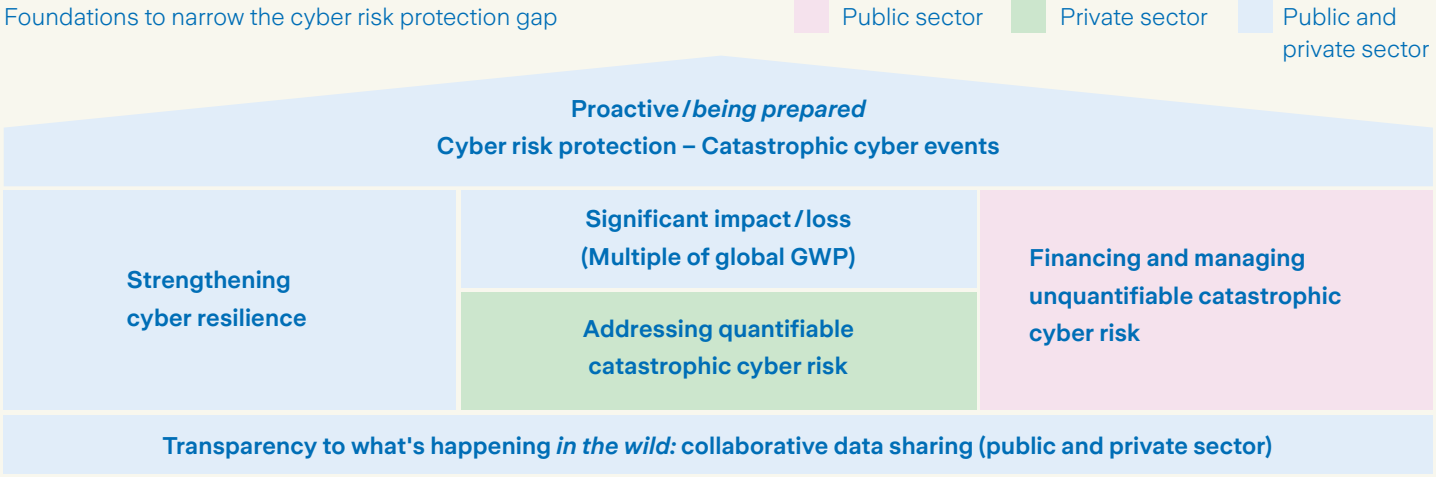
(3) Financing and managing unquantifiable cyber risk, which essentially is uninsurable, requires public sector-led solutions alongside public-private partnerships to sustain the market and broader economy as catastrophic incidents arise.

However, all of this will not be enough without shedding light on what is happening *in the wild* and making it transparent. Underneath this three-pronged strategy, it is imperative to build a knowledge base as its foundation by devising easily accessible metrics at the aggregate level that would need to go beyond cyber loss data.

The metrics outlined in this paper can be an important step in reducing the cyber risk protection gap. Quantitative data provides a solid foundation for improving existing frameworks, standards, guidelines, and best practices for managing cyber security risk.

Clear, actionable metrics allow us to quantify economic harm from cyber incidents, better evaluate the effectiveness of the cyber insurance market, and track the impact of cyber regulations. They enable benchmarking and shared learning.

Illustration 1
Foundations to narrow the cyber risk protection gap



In case of a cyber event materializing, the metrics outlined in this paper could further help determine whether crucial trigger points or thresholds, as implied by illustration 1, were met or surpassed. This, in turn, could be used to classify cyber events according to the extent of their catastrophic consequences, similar to how the Richter scale allows a comparison and classification of the size of earthquakes.

While such a classification in itself would not seem to be of much use in preventing an incident from happening, it could still lead over time to the establishment of officially recognized parameters on which to base predetermined action by public and private sector parties. In supporting the development of insurance policy wordings aligned with those classifications, it could even result in parametric insurance solutions being deployed to protect against cyber risks.[1]

[1] Parametric insurance is a type of insurance that pays out a predetermined amount based on the occurrence of a specific event, rather than the actual loss incurred. The payout is triggered when measurable parameters – e.g., rainfall levels, wind speed, or earthquake magnitude – exceed a defined threshold.

Section 2

Completing the picture: Data beyond cyber incident reporting

Current cyber regulations *(see box 1: EU use case and gap analysis, as an example)* have to a large extent been focused on creating requirements for reporting cyber incidents once they have happened. Most reporting at national level captures loss events – incidents that have already resulted in harm. While there are moves towards pre-breach requirements such as strengthening the resilience of digital products, the cyber threat landscape is in the meantime rapidly evolving.

Ransomware remains a top threat, with attackers adopting new tactics and technologies. It increasingly includes the use of artificial intelligence (AI) or targeting suppliers and service providers to exploit supply chain vulnerabilities and compromise large organizations.[2] Cyber threats are becoming ever more sophisticated and targeted, thereby outpacing the scope of currently available information necessary to appropriately shape pre-breach requirements.

At the same time, the scope of those targeted by cyber attacks is also significantly widening due to AI-powered tools, the proliferation of Ransomware-as-a-Service, and ever more digital touchpoints across the economy.[3] As only some organizations, products and services are covered by the current reporting requirements, the resulting shortfall in valuable cyber threat insights from existing cyber incident data is constantly growing.

Holistic data collection

To fully understand a country's cyber resilience, including the status of public and private organizations across industry sectors and market segments, current incident reporting is not sufficient for informed decision-making. A more holistic and proactive approach to data collection is required.

Focusing solely on loss events limits cyber risk understanding, as it misses critical insights into the broader threat landscape. Using metrics, which blend in a wider range of indicators such as the ratio of threats to actual losses, organizational exposures, cyber hygiene practices, and systemic weaknesses, enable to gain a clearer, proactive view of vulnerabilities and risk posture. Metrics that reflect such a broader approach at the aggregate level enable earlier detection of issues, more effective prioritization of resources, and collective action against widespread threats.

[2] CyberProof's Mid-Year Threat Landscape Report (2025) highlights a 38 percent year-over-year increase in enterprise ransomware incidents, while GuidePoint Security's GRIT Q2 2025 Report identifies 71 active ransomware groups, a 58 percent increase from the previous year.

[3] Examples for this are provided by ESET Research.(2025). PromptLock: The First AI-Powered Ransomware or Veeam. (2025). Supply Chain Ransomware Report.

When an event translates into an incident, additional pieces of information are uncovered and can become important to understanding the wider threat picture. What was the root cause? What vulnerabilities were exploited? Was it a single point of failure?

The recently proposed cyber security metrics from The European Financial Services Round Table (EFR) go exactly in that direction, being designed to improve the resilience of the European financial sector. However, these are intended for the Board and C-level senior management at financial institutions and are not country-level initiatives.

The EU's Network and Information Security Directive 2 (NIS2) as well as the Digital Operational Resilience Act (DORA), both applicable since late 2024/early 2025, require the submission of such information as part of a detailed incident report. However, further insights could be inferred from the tactics and technologies used in a cyber incident, in particular from the patterns that emerge when grouping those attacks according to threat actors and the targets' characteristics such as company size, industry sectors, market segments or infrastructures (public/private).

Aggregating these data points into consistent cyber security metrics at national level would not only enable meaningful comparisons with existing protections, allowing policymakers to identify where they might need to be enhanced. It could also be used to reveal how the frequency and impact of threats and losses correlate with an economy's GDP and the capacity to afford robust cyber defenses. The gap between the frequency of threat events and actual losses provides valuable insight into the strength of cyber security measures. Granular data providing these insights will be critical for informed, strategic decision-making to address specific vulnerabilities and enhance overall national cyber resilience. Standardized metrics will ensure these data insights are readily accessible.

Section 3

Proposed metrics

Looking across the range of potential data points that could be usefully tracked, we propose six key metrics for adoption. These are aligned with the six functions or dimensions in the U.S. National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF), building therefore off an existing body of knowledge.

The proposed metrics are not intended to provide an exhaustive and comprehensive picture of the associated CSF functions. Rather, they were selected as easy to read and easy to interpret indicators that will signal whether a country's cyber resilience is improving or deteriorating as far as the portrayed dimensions are concerned. As experience and research progress over time, these metrics should evolve, allowing for a more sophisticated para-metrization to reflect the cyber health status of a country and its digital infrastructure.

1. Percentage of organizations with cyber insurance or audit certification

This metric, looking at the general level of preparedness against cyber threats, would provide insight into organizations' understanding of their cyber security environment, including assets, policies and practices. Having cyber insurance or being subject to audit procedures and requirements such as SOC2[4] will drive this awareness and signal how effectively a nation's digital environment is identified and assessed. Data collection could rely on a combination of industry surveys, market research, and official certification databases. This figure could be further broken down by sectors and company size, revealing sector-specific insight levels and highlighting market segments that could be particularly at risk.

2. Proportion of exploited vulnerabilities older than one year

This metric covers the ability to safeguard assets and lower the likelihood and impact of adverse events. A better protected ecosystem would have fewer vulnerabilities overall, newly discovered vulnerabilities would be remediated more quickly, and malicious actors would see themselves in a rush to use newly discovered vulnerabilities more rapidly. In such a context, the proportion of exploited vulnerabilities older than one year provides a useful indicator for the strength of ecosystem defenses. As the proportion of old exploited vulnerabilities decreases, the more effectively protected the eco-system is. Admittedly, one year is an arbitrary cutoff which may appear to err on the longer side by some standards. However, more important is the underlying concept which is the ratio of old vulnerabilities to new vulnerabilities. The cutoff could be adjusted in the future as defenses improve. Data collection would need to combine threat intelligence data, vulnerability age analysis, and geolocation attribution of threat actors or affected systems.

[4] SOC2 (System and Organization Controls 2) is a framework based on five *trust service criteria* developed by the American Institute of Certified Public Accountants (AICPA) in 2011 for managing customer data, including cyber security and data protection dimensions. While the ISO 27001 audit is more widely used, it is only done at a specific point in time. SOC2 is for a period (minimum six months) and therefore gives more guarantees.

3. Number of significant cyber incidents

This metric reflects the timely detection and analysis of cyber incidents. From a country-level perspective, not all events matter equally. Governments need to define what constitutes a significant cyber incident, whether in terms of economic damage or number of affected citizens.[5] The more successful a country becomes in effectively anticipating and detecting any cyber incident, the lower the number of significant incidents will be in a given time period. Data collection to establish this indicator would need to rely on public databases, governmental reports, and cyber security trackers.

4. Average time to containment of cyber incidents

This metric shows a country's ability to contain the effects of a cyber incident. Time to containment is defined as the duration between the first activity of a cyber incident and the point at which the threat is fully contained and can no longer spread. It includes both the ability to stop an ongoing event and the capability to assist affected organizations. The objective is for this timeline to be as short as possible across the economy and all organizations. To establish the average time to containment of cyber incidents at the country level, a combination of incident response metrics, regional benchmarks, and standardized definitions is required.

5. Mean time to restore operations

This metric assesses the restoration of normal operations after a cyber incident, referring to the average duration from the moment a cyber incident is detected until full operational functionality is restored. Since cyber disruptions degrade national security, economic prosperity, and public health and safety, the goal is to restore normal operations as quickly as possible. To collect this kind of information, it would take a combination of incident recovery metrics, regional benchmarks, and sector-specific data. This metric should not be confused with already existing operational risk regulations such as DORA in the EU. Their objective is to legally establish maximum time requirements to recovery for critical operations.

6. Percentage of unfilled cyber security positions

With this metric, we cover the governance aspect, which, in general terms, focuses on having effective legal and policy frameworks to incentivize cyber security, and ensuring that the country has sufficient cyber security capabilities – starting with qualified personnel – to manage its risk. Although this metric encompasses many types of activities, a country will already have difficulty governing its cyber activities effectively if, across the economy, job positions with such a profile remain unfilled due to a lack of qualified personnel. Some of those cyber security-specific positions may be required by regulation, while companies will also independently seek to create such positions and try to fill them. Establishing country-level vacancy percentages will require a gathering of workforce data such as the number of cyber security personnel employed and the number of open cyber security positions.

[5] From an insurer's perspective, a cyber incident could be defined as significant when corresponding to an unquantifiable (=non-insurable) catastrophic cyber event arising out of cyber warfare, or in case of a loss event magnitude that is a multiple (e.g., 250 percent and more) of the overall global gross written premium volume for quantifiable (=insurable) losses (also see illustration 1).

Collecting the metrics

At the country level, there is often no clearly stated assignation of roles and responsibilities regarding collection of cyber-related data. Long-standing data-gathering bodies such as traditional statistics offices don't lend themselves particularly well to obtain broader, proactive metrics that allow earlier detection of emerging risks. This results in a lack of standardized, sector-wide, and aggregated data, making it difficult to compare across industries, countries or regions. We need effective institutions in place to collect those benchmarks. To overcome this gap, we propose establishing dedicated National Cyber Statistics Bureaus and tasking them with establishing a comprehensive real-time view of a country's cyber health. While there have been formal proposals to establish national cyber statistics bureaus, particularly in the U.S., no country has yet fully implemented a dedicated national bureau solely for cyber statistics.

A National Cyber Statistics Bureau would:

- Ensure consistent and reliable cyber incident reporting.
- Continuously track cyber incidents, defenses, and digital resilience.
- Publish data and analyses.
- Evaluate the effectiveness of cyber security regulations.

With national cyber statistics bureaus in place at the national level, it would be possible to aggregate their findings through a supra-national body, adding a further layer of comparative information that can be exploited to spotlight critical developments in the global cyber threat landscape.

A global Cyber Statistics Organization could bring additional benefits such as:

- Maintaining a cyber statistics repository.
- Issuing timely global cyber alerts.
- Facilitating international cooperation on incident reporting and response.
- Promoting alignment of global cyber security standards, including shared ontologies, consistent definitions, and standardized measurement methodologies.
- Potentially declaring and sizing catastrophic cyber events to trigger predetermined actions by different public and private sector parties.

Existing institutions, such as the UK's National Cyber Security Centre (NCSC) or ENISA in Europe, could serve as partial templates for these entities but there is a clear need to establish dedicated capabilities to collect and aggregate cyber-related data points, and for policymakers to adapt existing requirements and regulations to support this.

Visualizing the metrics

Effective use of metrics requires user-friendly visualizations. Governments can establish baselines, test feasible reporting frequencies, and gauge reliability, creating a feedback loop to improve the utility of these metrics. Visualizations help decision-makers, organizations, and citizens understand cyber health and hold governments accountable.

A simple scorecard showing the metric, target, status, and change since the last report, color-coded by a defined algorithm, can be effective.

Table 1: Scorecard – values are purely an illustrative example

CSF Element	Measure	Target	Status	Change since last report
Identification	Percentage of organizations with cyber insurance or audit certification		G	N/A
Protection	Percentage of exploited vulnerabilities > 1 year	25%	35	-0.2
Detection	Number of significant cyber incidents	4	7	+3
Response	Mean time to containment (days)	2.5	4.0	-0.3
Recovery	Mean time to recover from an incident (days)	7	21	-4
Governance	Number of unfilled cyber positions	10,000	120,000	-500

Box 1

Case study: Data gaps in the EU's cyber incident reporting regulations

Sound cyber security metrics help countries stay ahead of breaches, while demonstrating the value of their security measures. By way of comparison, table 2 looks at the EU's current cyber incident reporting regulations summarized in the appendix of this paper. It examines the extent to which the data points required to establish the proposed metrics within the six categories are being currently already collected and aggregated at the EU level.

The main conclusion can be seen in the column on the right. Currently existing cyber incident reporting regulations in the EU are only to a very limited degree gathering the data necessary for a shift to proactive, holistic reporting, revealing notable gaps that would need to be covered.

Out of six metrics, only one (Detection) is covered fully, and in the case of two others (Response and Recovery), the data delivered covers it only partially. For three core functions (Identification, Protection and Governance), EU incident reporting requirements do not result in data points that would allow for the calculation of the proposed metrics.

In addition, various bodies are involved in collecting this mostly incomplete data and they are not necessarily sharing information with each other. All of the advantages that we cite about the creation of National Cyber Statistics Bureaus and a Global Cyber Statistics Organization are lacking.

To reiterate, just focusing on cyber incidence reporting data is not providing the full picture that would enable smarter risk management, support industry-wide cyber resilience, and reduce the chance of being blindsided by the next big incident.

Table 2: Data gaps in the EU's cyber incident reporting regulations

CSF Element	Measure	Data already collected	Data required for key metrics	EU incident reporting requirements (details see appendix)
Identification	Percentage of organizations with cyber insurance or audit certification	Fragmented	Yes	No
Protection	Percentage of exploited vulnerabilities > 1 year		Yes	No
Detection	Number of significant cyber incidents		Yes	Yes
Response	Mean time to containment (days)		Yes	Partially
Recovery	Mean time to recover from an incident		Yes	Partially
Governance	Percentage of unfilled cyber positions		Yes	No
Reporting	Independent body with full access to all data		Yes	Various bodies, but no data sharing

Section 4

Conclusion and call for action

As pointed out at the beginning, collaboration between governments and the private sector is essential. The private sector must actively collaborate with governments to develop a consistent set of national cyber metrics. This is a strategic opportunity to reduce systemic risk, improve cyber resilience, and enable smarter policy and investment decisions.

Cyber threats are evolving rapidly. Emerging technologies – AI, cloud, blockchain – are introducing complex vulnerabilities across the economy. Yet, most countries lack the data infrastructure to understand and respond effectively. Without standardized metrics, governments and businesses operate in the dark, risking costly delays and fragmented responses.

We claim there is a distinct gap between the impact of the evolving cyber threat landscape on a country's resilience, the insights drawn from current data collection, and the critical information still needed to address emerging challenges.

To overcome this gap and help build a meaningful national cyber risk picture, we suggest six core metricts that should be tracked:

1. **Cyber insurance/audit certification coverage –** percentage of covered organizations
2. **Vulnerability exposure rates –** percentage of exploited vulnerabilities older than one year
3. **Significant cyber incidents –** number of major breaches or attacks
4. **Time to containment –** average duration to isolate threats
5. **Time to restore operations –** mean time to full recovery
6. **Unfilled cyber security positions –** percentage of cyber security personnel vacancies

This will not happen without a dedicated effort. We call on policymakers to deliver on the following three actions:

1. Collaborate on data collection
Shift from reactive incident reporting to proactive, cross-sector data sharing. Leverage Computer Emergency Response Teams (CERTs)[6] and industry associations to coordinate efforts.

2. Establish dedicated entities
Create or empower national and global institutions to collect, analyze and report cyber statistics across industries and borders. Existing models like ENISA and NCSC offer partial templates.

3. Harmonize standards and frameworks
Convene stakeholders to align definitions, benchmarks, and reporting protocols. Organizations like ISACA (formerly known as the Information Systems Audit and Control Association)[7] may be able to help guide this process.

[6] CERTs are expert groups that manage cyber security incidents, provide threat intelligence, and coordinate responses. They exist globally at national, regional, sectoral and organizational levels – such as US-CERT, GovCERT.ch (Switzerland), and JPCERT/CC (Japan) – and often collaborate through networks like FIRST.org and ENISA.

[7] ISACA is a global professional association focused on IT governance, risk management, cyber security, and assurance. It supports professionals and organizations in achieving trust in and value from information and technology with certifications, frameworks, education/training, and research.

Appendix

EU regulation - cyber incident reporting

		GDPR	EU Cyber Resilience Act	NIS2 (Network and Information Security Directive 2)	DORA
When	Trigger	Personal data breaches.	Security breaches and exploited vulnerabilities affecting security of products with digital elements.	Reporting is required for incidents that significantly impact the provision of services or recipients. This includes incidents that have caused or are capable of causing severe operational disruption or financial loss.	Reporting required for major ICT-related incident. The incident affects critical services and the materiality threshold for data losses or two or more of the materiality thresholds criteria are met.
	Threshold	Breach likely to result in a risk to the rights and freedoms (Art. 33).	Incident likely to cause significant disruption or pose substantial risk to users or other.	An incident is considered significant if it: - Has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned. - Has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.	**The incident has had any impact on critical services.** **a)** >10% of all clients using the affected service. **b)** >100 000 clients using the affected service. **c)** >30% of all financial counterparts used by the financial entity (FE) **d)** >10% of the daily average number of transactions. **e)** >10% of the daily average amount of transactions. **f)** Any identified impact on clients or financial counterpart identified by the FE as relevant. **Material threshold for data loss.** Any successful, malicious and unauthorized access that occurs to network and information system, where such access may result in data losses.

Who	Market segment	All data controllers and processors across sectors, relevant for insurance due to sensitive personal data processing.	Manufacturers, importers and distributors of products with digital elements, essentially any hardware or software product that has a direct or indirect data connection and is sold on the EU market.	The NIS2 directive impacts a wide range of market segments, categorized into "essential" entities (sectors of high criticality), e.g., energy, transport, banking, health, or digital infrastructure, and "important" entities (other critical sectors), e.g., postal services, waste management, or food business.	The primary reporting obligation falls on "financial entities" including banks, credit institutions, payment institutions, investment firms, crypto-asset service providers, insurance companies.
	Person within the organization	Data Protection Officer (DPO) or legal person/team in charge of compliance activities.	Cyber Security Officer or designated compliance contact.	The management body of the entity is responsible for overseeing and approving cyber security measures. This means the ultimate responsibility lies with the top management. However, the actual task of reporting incidents is typically delegated to specific roles within the organization, such as CISO, IT Security Manager or Compliance Officer.	The legislation specifies that at least major ICT-related incidents are reported to relevant senior management. Entity to designate a primary and secondary contact person within the organization.
How	Template	Online notification tool of personal data breach (to relevant authority).	Reports submitted to national market surveillance authority (ANSSI) within 24 hours; harmonized format under EU standards.	The directive does not specify a universal template, but entities must provide detailed information about the incident.	The ESAs will develop common draft implementing technical standards to establish standardized templates, forms, and procedures for reporting major ICT-related incidents.

How	Timeline	Notification to relevant authority within 72 hours of awareness about the breach.	Notification to market surveillance authority within 24 hours of becoming aware of active exploitation.	Initial notification within 24 hours, followed by a detailed report within 72 hours.	**Initial Report:** As early as possible within four hours from the moment the incident is classified as major. No later than 24 hours from the moment the financial entity has become aware of the incident. **Intermediate Report:** The latest within 72 hours from the submission of the initial notification. Financial entities shall submit without undue delay an updated intermediate report, in any case, when regular activities have been recovered. **Final Report:** No later than one month from the submission of the latest updated intermediate report.
To Whom	ENISA	No direct notification to ENISA under the GDPR.	Must report to ENISA in case of severe cyber incident affecting the security of a product with digital elements or if a vulnerability is actively exploited. May receive anonymized summaries for risk analysis and coordination.	The detailed incident report does not need to be directly submitted to ENISA.	The detailed incident report does not need to be directly submitted to ENISA.
	National regulator	Commission nationale de l'informatique et des libertés (CNIL).	Agence nationale de la sécurité des systèmes d'information (ANSSI) – for smaller incidents & Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT - FR) for technical incidents.	Reports must be submitted to the relevant National Competent Authority (NCA) or Computer Security Incident Response Team (CSIRT).	Financial entities report to their relevant competent authority.

What					
	List of most important data points to report on	Description of the breach, (if possible) categories and number of data subjects impacted, type of personal data.	Product type, incident description, impact, Common Vulnerabilities and Exposures (CVE) identifiers, corrective actions taken.	The detailed incident report required within 72 hours must include the following information: **1.** Detailed description of the incident. - nature and specifics of the incident. - severity and impact of the incident. **2.** Type of threat or root cause. **3.** Indicators of compromise. **4.** Mitigation measures. **5.** Cross-border impact. **6.** Status update. **7.** Final report - not later than one month after submission of the incident notification.	**General Information about the Financial Entity:** Type of report (initial, intermediate, final) Name and Legal Entity Identifier (LEI) code of the financial entity. Type of entity under Digital Operational Resilience Act (DORA). **Content of Initial Notification:** Incident reference code. Date and time of detection and classification. Description of the incident. Classification criteria triggered. Member states impacted. How the incident was discovered. Origin of the incident. Business continuity plan activation. Reclassification (major to non-major). **Content of Intermediate Report:** Incident reference code (competent authority provided). Date and time of occurrence. Date and time of regular activities restored. Classification criteria. Type of incident. Threats and techniques used. Affected functional areas and business processes. Affected infrastructure components. Impact on financial interest of clients. Reporting to other authorities. Temporary actions/ measures taken. Indicators of compromise.

What	List of most important data points to report on				**Content of Final Report:** Root causes of the incident. Dates and times of resolution and root cause addressed. Incident resolution. Information relevant for resolution authorities. Direct and indirect costs and losses. Financial recoveries. Recurring incidents. **Cyber Threat:** General information about the reporting entity. Date and time of detection of the threat. Description of the threat. Potential impact on the financial entity and its clients. Classification criteria that would trigger a major incident report. Status of the cyber threat. Actions taken to prevent materialization. Notification to other financial entities or authorities. Indicators of compromise. **Data Loss Details:** Type of data losses (availability, authenticity, integrity, confidentiality). Description of the data losses. **Impact Details:** Number and percentage of clients and financial counterparts affected. Impact on relevant clients or financial counterparts. Number and value of affected transactions. Reputational impact. **Downtime Details:** Duration of the incident. Service downtime. **Other Incident Details:** Description of impact in other member states. Types of impact in the member states.

In force		In force since 2018.	Expected to apply from 2027 after transitional period post final adoption in 2024	The NIS2 directive entered into force on January 16, 2023. EU member states were required to transpose the directive into their national legislative frameworks by October 17, 2024. This means the specific requirements should be fully implemented and enforceable in each member state since October 2024.	DORA entered into force on January 16, 2023 and became applicable on 17 January, 2025.
Applicability	EU domiciled companies	Direct application to all companies operating in the EU and processing personal data (offering goods/ services or monitoring behavior).	Direct application to all EU-based manufacturers of critical digital products, sold/placed in the EU.	The directive applies to entities operating within the EU, including non-EU domiciled companies that provide services within the EU.	The directive applies to entities operating within the EU, including non-EU domiciled companies that provide services within the EU.

ZURICH

About Zurich – Zurich Insurance Group (Zurich) is a leading multi-line insurer serving people and businesses in more than 200 countries and territories. Founded 150 years ago, Zurich is transforming insurance. In addition to providing insurance protection, Zurich is increasingly offering prevention services such as those that promote wellbeing and enhance climate resilience. The Group has about 60,000 employees and is headquartered in Zurich, Switzerland. Further information is available on our website. **zurich.com**

CYBER THREAT ALLIANCE

About Cyber Threat Alliance – The Cyber Threat Alliance (CTA) is a nonprofit organization dedicated to strengthening global cyber security. By enabling near real-time sharing of high-quality cyber threat intelligence, CTA helps its 37+ members headquartered in 12 countries protect users, disrupt malicious actors, and improve digital resilience. Members collaborate through an automated platform and direct communication to share validated threat data, research, and response strategies. CTA fosters a trusted network for collaboration, supports global cyber security initiatives like the Ransomware Task Force, and promotes policies that enhance digital security. Through leadership, partnerships, and innovation, CTA plays a vital role in defending the global digital ecosystem. **cyberthreatalliance.org**

CyberGreen

About CyberGreen – The CyberGreen Institute (CyberGreen) is a U.S.-based 501(c)(3) non-profit organization advancing the discipline of Cyber Public Health by measuring systemic cyber risks. It develops global metrics and data-driven insights to help governments, researchers, and industry reduce harm across critical internet infrastructure. CyberGreen promotes evidence-based cyber security practices through research, public reporting, and cross-sector collaboration, aiming to build a safer and more resilient cyber ecosystem. Further information is available at **cybergreen.net**