IBM's comments on the NIS2 Directive transposition in the Netherlands

June 2024

The revised NIS2 Directive enhances the framework for cybersecurity collaboration, further raises cyber awareness, improves threat intelligence sharing capabilities and builds skills across the EU. Its implementation comes at a crucial time amid an unprecedented rise of cyberattacks globally, while Europe in particular was identified as the most targeted region in IBM X-Force Threat Intelligence Index 2024.

IBM is a leading provider of global hybrid cloud and AI solutions, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. Thousands of government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to achieve their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity and service.[1]

We welcome the draft Dutch law transposing the NIS2 Directive. The law strikes the right balance between the EU framework and the national implementation context. It also allocates and clarifies roles of both private and public entities that operate within the cybersecurity ecosystem in the Netherlands. Building on our experience servicing customers globally across the critical sectors, we would like to share some recommendations to further improve this legislation.

Incident notifications

Notification

Entities should be enabled to focus their limited security resources toward responding to the cyber attack and restoring operations. It is therefore important to focus reporting only on the relevant information that provides real operational insights. Therefore, we recommend that the Ministry clarifies that **interim reports are only required for material changes or updates**. This ensures that the entity can focus its resources on responding to the incident and restoring operations without dedicating important security resources to a formulaic reporting exercise.

[1] Visit www.ibm.com for more information.

In additon, in order to ensure legal clarity, we advise to measure the reproting timeline in days. For exmape, 30 days instead of 1 month, 90 days instead of 3 months.

Reporting in the B2B context

The law should more clearly allocate the **reporting responsibilities in the B2B context**, especially as some entities covered by the law are both critical infrastructure entities and the third-party service providers to critical infrastructure. The proposed draft legislation does not in the current language take into account the different roles and responsibilities of these entities which could lead to ambiguous and duplicative reporting obligations. If a covered entity is acting as a third-party service provider to a covered entity customer that is the victim of a reportable cyber incident, the law should be clear that the covered entity customer, and not the third-party service provider, is required to report.

Only the covered entity that was impacted by the cyber incident can assess the impact and gravity of such incident. Under the current proposal, a third-party service provider, such as a cloud provider or any other digital infrastructure provider deemed as essential, may have to report to the regulator about an incident that impacts its client without having the necessary information or overview of end users affected. We would thus recommend including a clarification in the proposed national NIS2 transposition law similar to that in Art. 16(5) of the original NIS Directive of 2016:

> *"[w]here an operator of essential services relies on a third-party digital service provider 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 digital service provider shall be notified by that operator."*

Reporting entry point

The proposed text should not create overly burdensome reporting obligations. Currently, the proposed text requires reporting the incident to both the CSIRT and the national competent authority. In the context of the emerging cybersecurity threat landscape, it is important to focus on streamlining the reporting process so that the information exchange is done in a the most efficient way possible, enabling both regulators and the reporting entity to prioritize limited resources on risk mitigation, rather than navigating myriad reporting obligations.

Requiring multiple reports to multiple regulators turns the incident reporting requirement into an unnecessarily bureaucratic exercise, forcing covered entity victims to shift limited resources to respond to overlapping regulatory obligations, rather than focusing on incident mitigation and restoring its critical infrastructure activities. **We therefore recommend that the notification goes into one point of entry – the national CSIRT**. The CSIRT can then share the information with the national competent authority (but not any other entity unless otherwise agreed by the reporting entity.)

It is also important to consider future implementation of other legal acts – like the CRA. Since many entities will be in scope for each of these horizontal frameworks, we recommend

designating the national CSIRT as the single point of entry for reporting both under the NIS2 and the CRA.

Thresholds

In order to develop a coherent and actionable threat intelligence sharing, the reporting **definitions and thresholds should be set at the EU level through the implementing act**. The following factors should be considered:

1) Material harm and severity. Reporting should be required for incidents that have a significant impact on critical services and that are likely to result in material harm to material business activities, national security, economic stability, or public health and safety. Factors may include:
    a) number of individuals or CI;
    b) data or systems involved;
    c) length of an outage or exposure;
    d) novelty of threat actor's approach;
    e) availability of back-up systems.
2) Malicious intent element. Consider requiring a "malicious intent" element to focus on real security threats.
3) Non-systemic and isolated incidents that are not caused by malicious activity should be excluded from notification obligation, unless they result in significant disruption of critical services or severe impact on human health.

Safe harbour

Liability exemptions or safe harbors for notifying incidents should be introduced in the transposition law, as a minimum in line with Article 23(1) of the NIS2 Directive. Covered entities experiencing a substantial cyber incident are targets and victims. A liability safe harbor would encourage entities to come forward early to share information. Providing strong confidentiality and liability protections for reporting entities will promote information sharing and partnership with the Dutch CSIRT and a national competent authority and avoid revictimizing the victim. **Liability protections for reporting entities help promote trust and encourage information sharing in a controlled and responsible way and assure reporting entities that the information they provide will not be used against them or be made public**.

Vulnerability disclosures

Promoting voluntary information sharing about threats and vulnerabilities helps promote better situational awareness and mitigation. It is important to ensure that this information is shared in a controlled way to enhance trust between the parties and encourage further collaboration. For example, Article 36 that addresses voluntary vulnerability disclosure should not mandate reporting of vulnerabilities through an intermediary and should allow researchers to also contact manufacturers directly, if they so choose.

Moreover, Article 32 and Article 35 should have additional clarification that **disclosure of information about threats, incidents and vulnerabilites can happen only after a mitigation measure is available and upon the consent of the concerned entity**.

Disclosure of incidents to service recipients

Article 32 should provide more precise language about sharing information about incidents with service recipients. Entities should notify service recipients about incidents that are significant and that will impact their service recipients. There are too many cybersecurity-related signals that entities already address daily and there is no benefit to inundating service recipients with additional superfluous information about threats and incidents that are not significant and that do not impact them.

This requirement should be limited to those cases when they are impacted and only when they need to take specific actions to mitigate such incidents. Otherwise, this requirement will overwhelm service recipients with unnecessary information and could discourage entities from disclosing incidents overall to avoid reputational harm. Moreover, **an additional clause should be added to the text to ensure that CSIRTs can share information about incidents with third parties – including service recipients – only upon the consent of the reporting entity**.

B2B Software & Support

Article 32 of the proposed legislation, which aims to implement Article 23(1) and (2) of the NIS2 Directive, appears to require software manufacturers to provide free software updates, patches and other software support services. While this proposal might make sense in the Business-to-Consumer (B2C) software environment, it fails to reflect the realities of the Business-to-Business (B2B) software ecosystem. The proposal improperly presumes that there is a very simple software licensing model, where the customer purchase once the software and any subscription and support services, but this not the cases for the vast majority of B2B customer license software. Unlike in a B2C environment, where software can be updated in a few minutes by accepting a push notification, upgrading and patching B2B systems is a significantly more complex process, customized to individual customer needs and configurations, and requires greater resources, expertise and the involvement of many more stakeholders.

The B2B software model involves transactions between sophisticated business customers and the software manufacturer. Generally speaking, **B2B customers customize their subscription and support services** for the software they purchase. Many customers choose to purchase software and handle the support and patching themselves so that they can manage updates to their complex environments according to their own needs and priorities; others may purchase the software, together with the manufacturer's subscription and support services for a specific period set forth in the software license agreement. A sophisticated B2B customer may intend to fully support the software on its own without any assistance from the software manufacturer. Article 32 of the Netherland's NIS2 transposition should not force such significant changes on the B2B software model, where sophisticated B2B market participants want to manage themselves how subscription and support services are currently provided.

Liability protections for information sharing

Article 17 (2)(b) provides that the CSIRT shall share early warnings, notifications and announcements, and disseminating information *"to the competent authorities and other relevant parties"* in near-real time. We strongly encourage the Ministry to reconsider this provision and **remove or limit the reference to "*other relevant parties"*** as this language is too broad and would significantly discourage entities from sharing information about incidents. The reported information should only be maintained by the CSIRT while further dissemination should be limited exclusively to the national competent authority and entities responsible for national security, as needed, with appropriate confidentiality and liability protections for covered entities.

Article 17 (3) provides that CSIRT may proactively and on non-intrusively scan a publicly accessible network and information system of an essential entity and significant entity. It is important to **clarify and define what "non-intrusive" implies**. Further parameters should be included in the text so that the scans are performed in a controlled manner – for example, providing a clear time range for these scans. Moreover, CSIRTs should notify entities prior to conducting the scans to avoid potential unexpected disruptions in their activities.

In addition, we recommend adding further clarification that the scans are conducted based on the fair assessment criteria:

> *"Member States shall ensure that the competent authorities, when exercising their supervisory tasks in relation to essential entities, have the power to subject those entities at least to: security scans **based on objective, non-discriminatory, fair and transparent risk assessment criteria**, where necessary with the cooperation of the entity concerned;"*

Moreover Article 39 should clarify that CSIRT or a competent authority can disclose information about incident "*after consultation **and upon the consent** of the entity concerned*".

Governance

We recognise that cybersecurity is integral to an entity's overall corporate risk management. Corporate management boards that oversee corporate risk management already consider cybersecurity risks when executing their duties. They coordinate closely with relevant subject matter experts responsible for cybersecurity to assess and mitigate cybersecurity risk as part of their overall corporate management duties. While it is important that corporate board members have knowledge of cybersecurity risks, requiring corporate boards to have specific detailed cybersecurity expertise and specific training is overly prescriptive and unnecessary.

Corporate management bodies of essential entities and significant entities already have IT security specialists that possess the necessary qualifications to develop and implement an entity's cybersecurity strategy. **The skills referenced in Article 26 (2) are very technical** and more appropriate for corporate security management personnel responsible for implementing cybersecurity risk mitigation, rather than corporate management board members. Reports by CISOs and IT security personnel already provide members of

corporate management bodies with sufficient information and in-depth insights to make informed decisions. **To really address the risk, it is more appropriate to require that covered entities have corporate governance programs that include cybersecurity risks and that place cybersecurity accountability and responsibility on the parties best placed to identify and mitigate the risks**.

Supervision of entities

We advise against "naming and shaming" practices; releasing publicly information about incidents or sharing such information with users without an entity's consent creates serious cybersecurity risks. In addition, such policies challenge trust between entities and CSIRTs/national competent authorities and undermine efforts to promote a transparent and proactive information sharing ecosystem.

In addition, before a regulator can penalize an entity for non-compliance or failure to report an incident, there should be a **cure period** for the entity to submit a compliant incident report. This will promote effective and efficient information sharing and will not penalize the victim.

Last but not least, we recommend amending the language in Article 70 by replacing "*after reasonable suspicion that the essential entity has not complied with the other or certain obligation under this law*" with "*where justified on the ground of an infringement of this Directive by an Essential Entity*" to better align with NIS2 Directive as well as to **promote partnership and coordination, rather than a punitive framework**.

Duty of care

IBM urges the Ministry to avoid creating a rigid list of prescriptive cybersecurity requirements that a covered entity must implement to comply with its duty of care obligations. Instead, we recommend that covered entities conduct a risk assessment to identify their unique cybersecurity risks and implement reasonable policies, controls, and practices to address such risks.

Covered entities should be able to meet their duty of care obligations by leveraging commonly accepted global standards for cybersecurity, secure product development, and supply chain integrity. Widely adopted global standards such as the SDDF, NIST SP 800-53, ISO 27001 and ISO 20243 already provide meaningful guidance and a strong foundation for effective cybersecurity policies and practices. Rather than develop new certification requirements, the law should leverage existing standards and conformance schemes to facilitate increased transparency and accountability regarding cybersecurity practices. Focusing resources on the consistent application of existing and common standards will result in better cybersecurity overall.