Brussels, 4 June 2020

EBF position on Cyber incident reporting

Proposals from the European banking sector for a harmonised reporting environment

KEY MESSAGES

This document aims to address the fragmentation of the EU cyber incident reporting framework, resulting from the existence of several different Incident Reporting Requirements across Europe, and to make proposals for regulators and policymakers for fostering information sharing and cooperation between Financial Institutions and Supervisory Authorities.

Depending on the type of incident, the reporting entity and the different legislations that apply, the current regulatory framework for incident reporting is characterised by:

- Different taxonomies;
- Different timelines, thresholds, information requirements and multiple templates for reporting;
- Various actors involved, from both the sender and receiver sides;
- Insufficient clarity in existing communication channels between public bodies and authorities (e.g. Europol, national law enforcement, national financial regulatory bodies, national CERTs).

These elements create additional regulatory and operational burdens that financial institutions have to abide by during or immediately after having suffered a cyber incident[1]. They also prevent the creation of more centralised and uniform mechanisms that can speed up the reporting process and enable a smoother exchange of information and good practices. Due to the complex rules and reporting channels, existing different requirements result in coordination and compliance challenges.

[1] A cyber incident for the purposes of this paper should be considered as encompassing the definitions of: NISD, GDPR, PSD2, eIDAS.

In order to ensure that financial institutions are able to quickly and effectively report cyber incidents without at the same time sacrificing a proper incident management and recovery process, and very much in line with the ESAs Joint Advice on legislative improvements[2], the European Banking Federation (EBF) makes the following proposals for supervisors and regulators:

- **Establish a central reporting and coordination hub in each Member State;**
- **Harmonise reporting thresholds and create a common taxonomy for cyber security incidents**;
- **Foster public-private real-time collaboration between regulators, supervisors, law enforcement, financial institutions and other cross-sectoral infrastructure actors;**
- **Further involve national CERTs in information sharing**;
- **Introduce a regular bi-directional information flow between regulators/supervisors and the industry.**

1 Introduction

The continuous evolution of the regulatory framework touching upon cybersecurity topics represents both a response to cyber risks and a challenge when it comes to financial institutions. A number of regulatory acts have introduced new requirements in data security, information sharing, incident reporting and crisis management. The acts and frameworks for incident reporting foresee the involvement of multiple authorities at national and European levels, encompassing different procedures and templates, creating overlaps and redundancies in the process of incident reporting.

Consequently, a single incident might entail the need to report to different supervisory authorities, complying with the applicable impact assessment details and thresholds, timeline, data set, and communication means. All these different criteria and patterns cause fragmentation with respect to the overall incident reporting requirements and are to be managed along the critical path of handling the incident itself. As proposed also by the ESAs, the existing incident reporting requirements should be streamlined by clarifying any overlapping provisions and standardising reporting instruments. In fact, a clear set of harmonized rules, including timeframes, taxonomy and thresholds would be beneficial so that the industry can comply properly and smoothly with incident reporting requirements.

A harmonised incident reporting model would boost clarity on an incident, adequate sharing of information and a trusted cooperation between stakeholders, while at the same time would adequately respond to the need of different authorities to be informed.

[2] Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector (10 April 2019).

Representing cybersecurity experts from national banking associations and big banks of 25 countries[3], the EBF Cybersecurity Working Group (CSWG) actively supports, through this paper and its regular work, the harmonisation of cyber incident reporting frameworks applicable in the financial sector to facilitate compliance on the part of reporting entities and allow them to better allocate resources in the actual tackling of cyber incidents.

In the following pages, we illustrate the major incident reporting requirements for the financial sector and financial market infrastructures (FMIs) under EU law. Then, we address the fragmentation of related requirements, resulting from differences between EU Regulations and Directives, and conclude by offering concrete proposals to address this challenge.

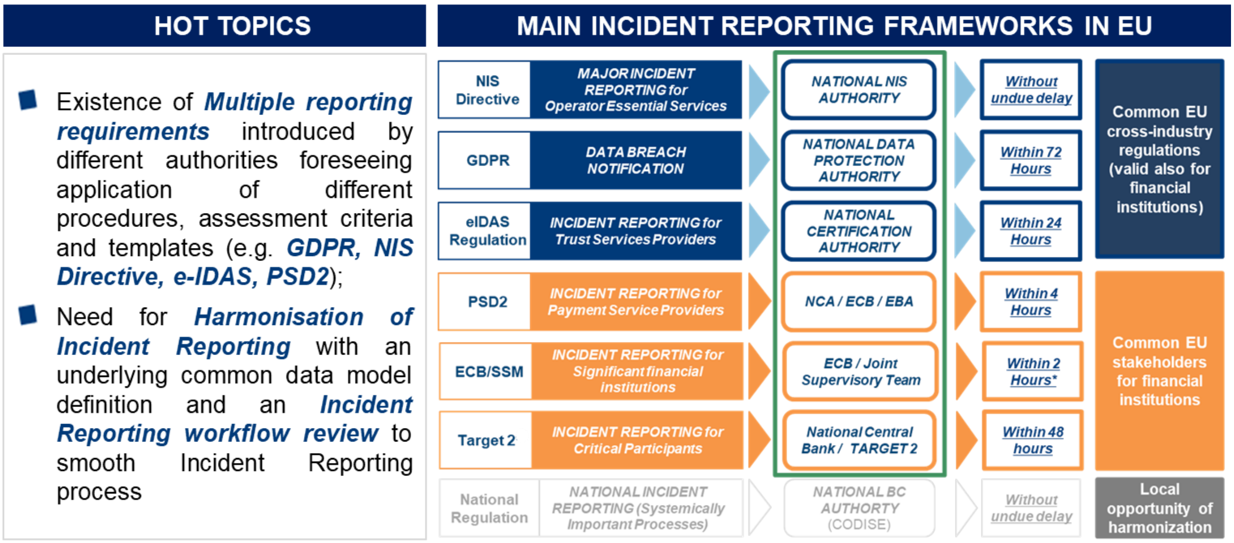
2 The major regulatory requirements on incident reporting across Europe for the financial sector and FMIs

Cybersecurity is a top priority on the EU agenda and a growing challenge for both the public and private sectors. The financial sector is taking a forward-looking approach to increase overall resilience to cyber threats rather than merely comply with existing and future requirements. All financial entities have to comply with EU incident reporting requirements and at the same time manage further requirements arising from their involvement in different national and international FMIs, even beyond the EU.

Incident reporting provides input valuable for an improved and more efficient cyber-risk governance with better prioritization of security measures. It is required by many regulations because it lies on the critical path of Incident Management, Recovery and Response as a milestone for the protection of customers' data but also an organization's information and reputation.

The illustration below, which is non-exhaustive, looks into EU law and the requirements provided for in different regulations:

[3] The EBF CSWG expresses its deepest appreciation to Intesa Sanpaolo for having provided their White Paper "*Building upon Incident Reporting towards enhanced cyber-resilience*", as a basis in elaborating the present EBF position paper on cyber incident reporting.



HOT TOPICS

- Existence of ***Multiple reporting requirements*** introduced by different authorities foreseeing application of different procedures, assessment criteria and templates (e.g. ***GDPR, NIS Directive, e-IDAS, PSD2***);
- Need for ***Harmonisation of Incident Reporting*** with an underlying common data model definition and an ***Incident Reporting workflow review*** to smooth Incident Reporting process

MAIN INCIDENT REPORTING FRAMEWORKS IN EU

NIS Directive	MAJOR INCIDENT REPORTING for Operator Essential Services	NATIONAL NIS AUTHORITY	Without undue delay	Common EU cross-industry regulations (valid also for financial institutions)
GDPR	DATA BREACH NOTIFICATION	NATIONAL DATA PROTECTION AUTHORITY	Within 72 Hours	
eIDAS Regulation	INCIDENT REPORTING for Trust Services Providers	NATIONAL CERTIFICATION AUTHORITY	Within 24 Hours	
PSD2	INCIDENT REPORTING for Payment Service Providers	NCA / ECB / EBA	Within 4 Hours	Common EU stakeholders for financial institutions
ECB/SSM	INCIDENT REPORTING for Significant financial institutions	ECB / Joint Supervisory Team	Within 2 Hours*	
Target 2	INCIDENT REPORTING for Critical Participants	National Central Bank / TARGET 2	Within 48 hours	
National Regulation	NATIONAL INCIDENT REPORTING (Systemically Important Processes)	NATIONAL BC AUTHORITY (CODISE)	Without undue delay	Local opportunity of harmonization

Picture 1: Comparison among Incident Reporting schemes (source: ISP WP[4])

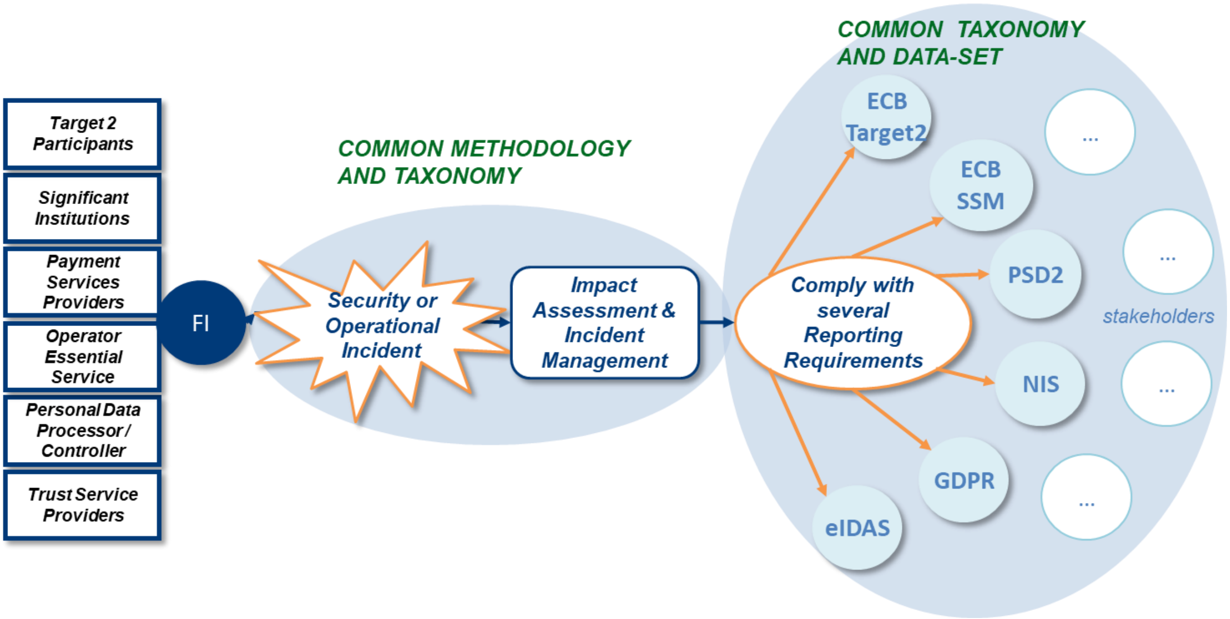
Picture 1 illustrates how financial institutions have to report significant incidents to multiple supervisors/authorities under different regulations (PSD2, ECB/Target 2, ECB/SSM, e-IDAS, NIS Directive and GDPR) in different timelines. Different thresholds, dataset templates and communication means are also added in this complex grid.

This fragmented landscape becomes even more challenging when considering that a cross-border institution which is present also outside of the EU has to take into account different reporting thresholds and comply additionally with requirements stemming from international and national regulations of the jurisdictions where the firms operate.

3 The fragmentation of incident reporting across jurisdictions and the possible scenarios

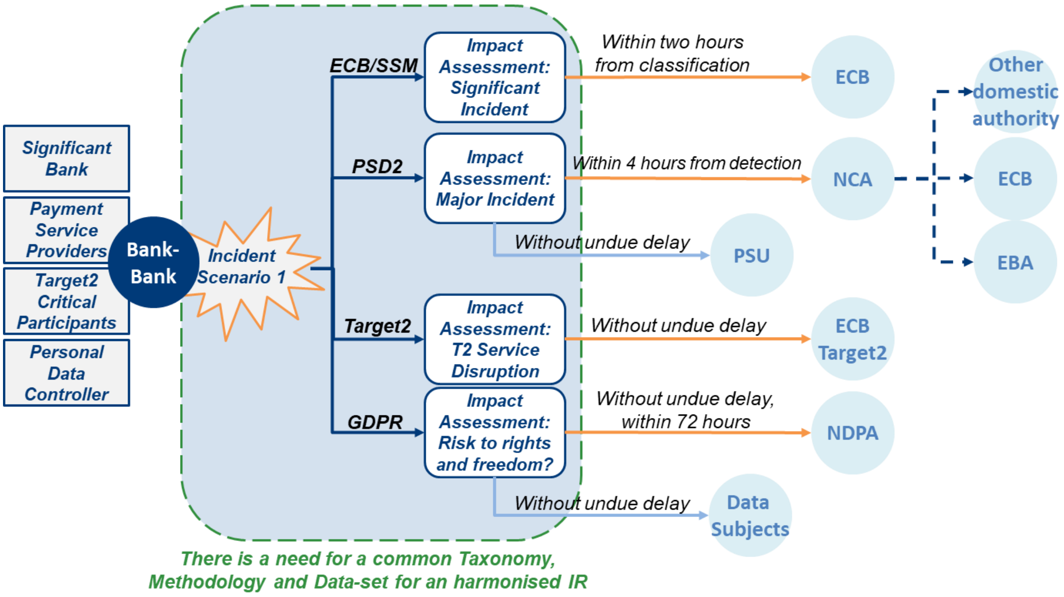
Once a cybersecurity incident occurs, a financial institution operating in the EU is expected to fulfill mandatory incident reporting requirements. Depending on the applicable regulation, the institution may be a "Significant Institution" under the ECB/SSM framework, a "Payment Service Provider" under PSD2, a "Target2 Critical Participant" for Target2, an "Operator of Essential Service" under the NIS Directive, a "Personal Data Processor/Controller" under the GDPR and/or a "Trust Service Provider" under e-IDAS.

[4] "ISP WP" stands for Intesa Sanpaolo White Paper on "*Building upon Incident Reporting towards enhanced cyber-resilience*"


COMMON TAXONOMY AND DATA-SET
Target 2 Participants
Significant Institutions
Payment Services Providers
Operator Essential Service
Personal Data Processor / Controller
Trust Service Providers
FI
COMMON METHODOLOGY AND TAXONOMY
Security or Operational Incident
Impact Assessment & Incident Management
Comply with several Reporting Requirements
ECB Target2
ECB SSM
PSD2
NIS
GDPR
eIDAS
...
...
...
...
stakeholders

Picture 2: Incident Reporting workflows high level overview (source: ISP WP)

Assuming that a financial institution called "Bank Bank" experiences an incident that falls into the framework of SSM, PSD2, GDPR and Target2, that financial institution will have to manage the following incident reporting workflows:


Significant Bank
Payment Service Providers
Target2 Critical Participants
Personal Data Controller
Bank-Bank
Incident Scenario 1
ECB/SSM
PSD2
Target2
GDPR
Impact Assessment: Significant Incident
Impact Assessment: Major Incident
Impact Assessment: T2 Service Disruption
Impact Assessment: Risk to rights and freedom?
Within two hours from classification
Within 4 hours from detection
Without undue delay
Without undue delay
Without undue delay, within 72 hours
Without undue delay
ECB
NCA
PSU
ECB Target2
NDPA
Data Subjects
Other domestic authority
ECB
EBA
There is a need for a common Taxonomy, Methodology and Data-set for an harmonised IR

Picture 3: Example of a possible scenario (1) workflow (source: ISP WP)

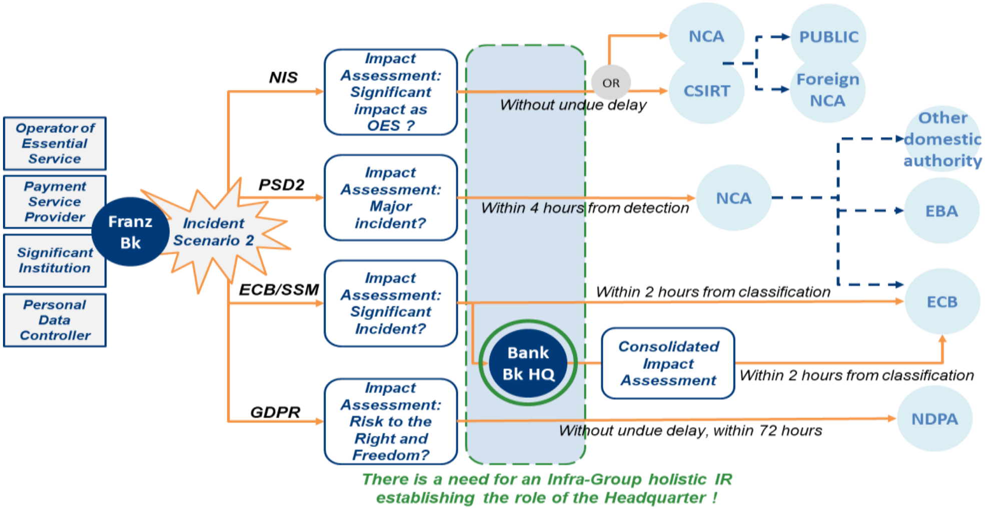
As mentioned previously, each regulatory framework sets its own rules with respect to thresholds, timeline for reporting and workflows with specific indication of the incident reporting recipient. This means that a multinational group needs to map all the processes and recipients of the incident reports, develop its own governance organisation and methodology, as well as a consistent process for handling cybersecurity critical events for all the locations it operates in. Things become more complex when considering that regulations often refer to a National Competent Authority, while the transposition of Directives could vary from one jurisdiction to another, adapting to national settings.

Moreover, large multinational financial institutions are present also outside Europe, having activities around the globe. In this case, it is possible that the underlying cultures influence the regulatory approaches as to the assets to be protected against cyberattacks as is the case, for example, with data protection.

Even when considering only the EU geographical scope, the approach of cross-border interaction is twofold. In a bottom-up perspective, each private entity has to assess which are the local jurisdictions applicable to its geographical presence. From a top-down perspective, in most cases legislators have identified a need for cross-border cooperation, however this relies upon the communication among National Competent Authorities, and most of the times legislations foresee a central entity at EU level that shall be informed by the National Competent Authority. In this respect, we see that several EU institutions are involved in incident reporting frameworks applicable in the financial sector: ECB, EBA, the EU Data Protection Board and the European Commission, ENISA, the CSIRTs Network and the Cooperation Group in addition to national competent authorities and regulators.

Therefore, on the one hand a financial institution shall address its incident reporting to several authorities, according to the type of incident and its impact. On the other hand, national and EU authorities, Member States and all other public stakeholders will have to ensure the exchange of information among themselves across jurisdictions.

Assuming that a multinational financial institution experiences a significant incident within its group that falls into the scope of NIS, PSD2, SSM, and GDPR, the financial institution will have to manage the following incident reporting workflows:


Operator of Essential Service
Payment Service Provider
Significant Institution
Personal Data Controller
Franz Bk
Incident Scenario 2
NIS
PSD2
ECB/SSM
GDPR
Impact Assessment: Significant Impact as OES ?
Impact Assessment: Major incident?
Impact Assessment: Significant Incident?
Impact Assessment: Risk to the Right and Freedom?
OR
Without undue delay
NCA
CSIRT
PUBLIC
Foreign NCA
Other domestic authority
Within 4 hours from detection
NCA
EBA
Within 2 hours from classification
ECB
Bank Bk HQ
Consolidated Impact Assessment
Within 2 hours from classification
Without undue delay, within 72 hours
NDPA
There is a need for an Infra-Group holistic IR establishing the role of the Headquarter !

Picture 4: Example of a possible scenario (2) workflow (source: ISP WP)

This demonstrates the pressure that these requirements put on the resources of financial institutions to deal with multiple reporting.

4 Possible approach for efficient and prompt incident reporting procedures

Financial institutions need to adopt tools and processes that allow them to be more efficient in handling simultaneously the management of an incident and the mandatory incident reporting requirements. The related frameworks often foresee a very tight timeline for incident notification. Generally speaking, the underlying notion is that reporting shall be undertaken without undue delay, and mostly within a few hours from detecting the incident itself. That means that the Incident Management Team has to take care of the incident management reporting in parallel with the incident management and recovery procedures. The need to report cyber incidents promptly and effectively vis-a-vis the urgency to implement mitigation and recovery measures shows how challenging the reporting process can be for financial institutions.

Time is a critical factor under these adverse circumstances, and this is why the preparation and readiness of the incident management team is of the utmost importance. Each private entity has to roll-out its own set of procedures and workflows, which could, for example, cover the following processes:

- Mapping the regulatory requirements on mandatory incident reporting that are applicable to the entity across all jurisdictions where it is active;
- Creating a governance framework to ensure a consolidated view in order to assess the impact of a single large incident spread across the multiple regions or legal entities, as much as identifying several smaller attacks against multiple entities of the Group across different jurisdictions;

- Developing a methodology embedding critical events classification, based on the incident impact assessment and its match with the multiple regulatory thresholds;
- Implementing tools that facilitate the handling of multiple, different incident reporting requirements;
- Mapping and managing the different templates and processes to ensure that incident reporting fulfils the required procedures, for example in terms of communication and encryption requirements.
- Establishing the secure communication channels with the regulators and supervisors;
- Complying with the different requirements in terms of pre-forensic or forensic analysis documentation.

5 EBF Recommendations

Cyber attacks are rapidly increasing and evolving in terms of targets, techniques and resulting impact for all kinds of institutions and businesses. At the same time, the regulatory landscape is evolving with the aim to support financial institutions in fighting cyber attacks, boosting cyber resilience and securing the whole ecosystem.

In this context and in light of the challenges raised by fragmentation in criteria and patterns under the main regulations for incident reporting, the EBF puts forward the following proposals:

- **Establish a central reporting hub in each Member State**. A centralised hub at national level could work as a one-stop shop mechanism, where all incidents, including sector-specific ones, can be reported. The national entity operating this hub would be the one responsible for the sound delivery of the requested information to each regulator, supervisor and/or law enforcement. A concrete and successful example of centralised reporting scheme is the Danish Joint Solution for reports on IT Security Events (FLIIS), described in the Annex below. As the harmonization of incident reporting is included in its mandate under the Cybersecurity Act, ENISA could further define such a mechanism and the EBF would be ready to provide more input in such a project. As an alternative to the constellation of national reporting hubs or as a next step, the EBF would also welcome the creation of a single and centralised EU reporting hub.
- **Harmonise reporting thresholds and create a common taxonomy for cyber security incidents**. By relying on common reporting thresholds and on the same definition of (cyber) security incidents in all regulations, the uncertainty of different interpretations would be alleviated and financial institutions would know exactly when and how they should report an incident. This clarity can be of great value especially for international organizations. Unifying all incident response obligations (to include continuity, data and security rather than just security) could also help in clarifying and aligning internal procedures and improve the resilience of the sector.

- **Foster public-private real-time collaboration between regulators, supervisors, law enforcement, financial institutions and other cross-sectoral infrastructure actors.** In light of the relationship between state and private critical infrastructures, there is a need to increase real-time collaboration in worst-case scenarios. This requires all stakeholders to be coordinated in handling crisis management procedures. There are several use cases around the world where this is done: FS ISAC and FS ARC in the US, Cyber Defense Alliance and Financial Sector Cyber Collaboration Centre in the UK, FI_ISAC in the Netherlands, and the Israel government with the private and public industry. We propose that a similar approach is implemented at the European Union level. It would facilitate better threat intel sharing and thus improve the sectors' capability to respond to incidents.
- **Further involve national CERTs in information sharing**. In order to facilitate the timely circulation of information across the financial sector and limit the propagation of cyber attacks and threats, the same reports sent to authorities could be shared, without additional burden for financial institutions, also with national and sectorial CERTs.
- **Introduce a regular bi-directional information flow between regulators/supervisors and the industry**. A two-way communication between authorities and industry would entail that authorities, after analysing and anonymising the incident reports, could provide back to the industry high-level guidance on threats, trends and mitigation recommendations. This would significantly help increase the sector's cyber resilience.

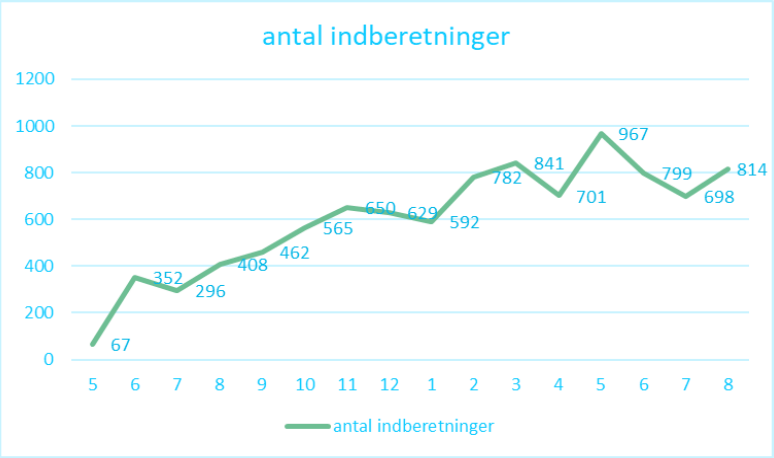
ANNEX

As previously indicated, the establishment of a centralised hub, aimed at collecting from financial institutions all reports covering incidents, and submitting them to the competent authorities, should be considered as the preferred model for reporting of cyber incidents. By fulfilling the above functions, the centralised hub would not only channel and coordinate the submission of reports more quickly and efficiently, but also indirectly facilitate the monitoring of cyber risks and trends at national level.

In this regard, the EBF would like to draw regulators' and supervisors' attention to a successful use case of centralised reporting hub: the Joint Solution for reports on IT Security Events (FLIIS), established by the Danish Government.

The FLIIS initiative emerged from the need for businesses to report IT security events through a single and safe digital platform, effectively and quickly. Based on the Danish national e-identification solution NEMID (easy ID) and relying on virk.dk, a digital service through which Danish businesses and citizens can already report relevant information to authorities using 1.500 different forms, FLIIS enables companies and individuals to submit reports of IT security events on time, including to the competent authority. Similarly, other businesses, in addition to Danish banks are major users of this reporting service.

After identifying and logging in via virk.dk, the reporter can select the regulation and the related competent authority under which he/she wants to submit a report. Several IT-related regulations (GDPR, NIS, PSD2, eIDAS, etc.) can be chosen and all the national competent authorities (DK Data Protection Agency, DK Business Authority, DK Financial Supervisory Authority, DK Cybersecurity Centre, etc.) are involved in the process.



Number of reports submitted

From May 2018 to September 2019 (included), over 10.000 reports were submitted by authorities and companies. More than 170 reports are submitted weekly, most of which are minor cases.

According to the most recent statistics, more than 60% of the incidents reported by all companies are data breaches, and therefore, related to GDPR.

Once the regulation(s) or the receiving authority/authorities has/have been selected by the reporter, a specific form to fill in will automatically appear. All the requested fields should be completed. For example: the reason for the incident (what happened), the timeline, others involved (if anyone), the severity of the incident, the consequences, and the handling. Almost all fields are mandatory for the first report and voluntary for those reports complementing the initial one. The full report will then be sent to all selected authorities via mail or web service.

Once submitted, a receipt with the related PDF document will be sent to the reporter, who will also be able to download the related PDF document. The data will be stored internally for 30 days.

Although the FLIIS mainly works as a safe gateway (not as an aggregation platform) and the entire processing phase is carried out by the receiving authorities in their own systems, this system, nevertheless, represents a safe and efficient dispatching solution, which makes it easier for companies and authorities to comply with the statutory reporting requirements, and contributes at the same time, to a clearer – albeit not fully complete - picture of the current IT security events.

For more information:

Alexandra Maniati
Director of Cybersecurity & Innovation
a.maniati@ebf.eu
+32 25083736

Sergio Tringali
Policy Adviser
s.tringali@ebf.eu
+32 25083724

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day.

www.ebf.eu @EBFeu