Q&A of Cybertips Webinar 'Reporting Your Cyber Incident: All You Need To Know'

By CCB Connect and Share

#	Question	Answer
1	How can we verify CCB is contacting us and not a vishing?	When we reach out unexpectedly, we understand that it can sometimes catch people off guard. So, to avoid any doubt, make sure you have our official email addresses and phone numbers on file: info@ccb.belgium.be or phone call +32 (0)2 501 05 60. If you're ever unsure about the legitimacy of a call, don't hesitate to call us back.
2	If there are only 4 aspects to report at the 24h mark, why is the CCB form asking for more information as mandatory fields?	According to the NIS law you need to provide indeed only 4 aspects in the 24h report. To make a proper assessment and priorities, the CCB is asking you to think about more then just the 4 obliged field. Of course, if you don't have the info yet you can indicate this with 'not known at this point in time'.
3	What about reporting of account compromise of any social media (or account duplicate like facebook) ? I guess linkedin hack could equally be harmful as email.	A compromized account can be reported to the concerned social network and the police. A NIS2 entity can report a compromized account of its staff to the CCB, should it be considered as an important cyberthreat. To solve the issue, we suggest that you take contact with the social platform where the account is hosted. Only the platforms themselves can give you back access to your account(s). All the platforms mentioned have 2FA options, which we suggest that you enable to be better secured against any account takeover.
4	Point of contact : should this be a generic coordinator overseeing the incident response process or a technical contact who is working on the resolution ?	It should be someone that's aware of the incident and understands its impact and who can answer basic technical questions about the incident to the CCB on behalf on the entity.
5	What is the purpose of reporting a security incident to the CCB?	Purposes are multiple: 1. to support the entity (when requested) with guidance and expertise that might prevent further damage OR help you recover faster. 2. to share the incident/technical info with others stakeholders within the same sector/cross-sector/EU level. Reporting isn't just about protecting your own organization- it helps strengthen cybersecurity across the country. If an attack goes unreported, it's not just your organization that's at risk. Other organizations could be vulnerable too. So, every report gives us valuable insights into emerging cyber threats, helping us better defend all Belgian organizations.
6	How can we make sure the confidentiality is ensured while sharing information ?	The information in the incident report form is secured during transit via encryption. If you prefer to send addtional sensitive information you can share with us via PGP encrypted mail. More info on how to do this can be found here: https://ccb.belgium.be/en/cert/send-encrypted-message
7	We recently started with a SOC. We would like to do a table-top DRP exercise to prepare us for when something would actually happen. Is it allowed to test the incident reporting with the CCB as well, by creating a test incident? (this way, we already know what steps to follow and can document this as well)	Answered live: We don't recommand to use the notification incident webform for exercice purposes (the person who is doing the notification has to sign that it is a true/real notification).
8	Belnet also has to report to BIPT. How do both reporting lines interact?	Belnet has to report according to the NIS2 law (to the CCB). The CCB will share it with BIPT. It's possible that, as an electronic communication provider, you have to report to BIPT as well (we both collaborate on incident handling).
9	If we have a mail compromised, or an user who clicked on a phishing link deleted some contacts in his Outlook.... this will not impact our daily operation, should we report this kind of incident ????	Question answered live: NIS2 organization should follow the criteria of the notification guide (for mandatory notification) and avoid non usefull notification: https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20EN.pdf.

10	Is there a template available with minimum reporting requirements in different notification stages? We'd like to know what needs to be supplied upfront and not during the incident.	The annex of the Incident NIS2 Notification Guide mentions all the information to provide during an incident notification: https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20EN.pdf.
11	Why do we not get a reference number when we do an initial notification of an incident? It is now difficult to provide add-on information about an already 'open' incident. I would add: Are there plans to have this? The reporting needed to be set-up really quickly, the CCB managed, so congrat. CCB has the example of SaveOnWeb, where a private company	Answered live: Thank you for your comment. It's useful to improve our reporting process.
12	If the company is operating in multiple european countries, how to determine which local authority should be informed? Depending of where the compromized device is, or should it be the country of the headquearter, or both ? thx	Answered live - NIS2 jurisdiction rules and the impact defined where to notifiy the incident: First of all, we refer to the NIS2 jurisdiction rules, in other words in which Member States you are subject to NIS2 legislation and consequently where the competent supervisory authorities are located: - General rule - establishment jurisdiction: jurisdiction of each Member State in which the entity has an establishment within the EU. - Exception 1 - Service location jurisdiction: entity falls under the jurisdiction of each Member State where they provide their services within the EU (for providers public electronic communication networks and services). - Exception 2 - Main establishment jurisdiction: entity falls under the jurisdiction of the Member State in which they have their main establishment in the union (for digital infrastructure and digital providers). - Exception 3 - Public administration jurisdiction: entity falls under the jurisdiction of the Member State which has established it. Next, you need to look in which Member States, under whose jurisdiction you fall, the incident has an impact. Finally, you must report the incident to the competent supervisory authority in those Member States (in Belgium this is the CCB).
13	The previous platform allowed us to view previous created incident. This new platform does not. Do you foresee to give us access to previously created incident ? Besides, when you created an incident you do not receive a copy of the details of created incident. Do you also foresee to change this ?	There are currently no plans for NIS2 organizations to see old incidents via the platform, but we welcome the suggestion and will look into ways to provide a copy after receiving a notification of a NIS2 incident at your organization.
14	In Belgium we need to notify the CCB, what about other countries and authorities if you are a global organization (perhaps with HQ in Belgium or somewhere else) and you have an incident with an impact on the activities in multiple countries... ?	The NIS2 jurisdiction rules and the impact of the incident define where to notifiy the incident. See question 12.
15	If a critical service is impacted outside of business hours, whom do we call? The national crisis center, CCB...?	The main CCB's phone number can be called at any time via +32 (0)2 501 05 60. Outside 9h30 - 16h30 your call will automatically be transferred to the NCCN. NIS2 entities can reach out to the CCB in case of a cybersecurity incident via the incident notification webform and/or phone call +32 (0)2 501 05 60). Critical infrastructures/ critical entities (CER) should inform the National Crisis Centre (NCCN) for all other incidents/aspects of the incident.
16	Do you ever get false incidents, to trap you away from attending to the true incidents? How do you mitigate this situation? I would guess you don’t have that many personnel	Our team is well-prepared and has protocols in place to verify the authenticity of incidents before deploying resources. Additionally, we continuously train our personnel to prioritize and manage incidents effectively, ensuring that genuine emergencies receive the attention they require.

17	Are there dedicated persons /institution as Belnet has the SCP (security contact persons)?	There is no dedicated contact person foreseen within the CCB. You can contact the CCB via incident@ccb.belgium.be or by calling +32 (0)2 501 05 60. Each NIS2 entity on its turn has to appoint a contact person for cybersecurity purposes. The contact person can be appointed in the SafeOnWeb portal.
18	Does the reporter of the incident have to identify him or herself via ID/ITSME just like when you'd register your company to the CCB for the NIS2 directive?	No there is no need to identify when reporting an incident to avoid obstacle in the notification process. We have protocols in place to verify the authenticity of incidents before deploying resources. The URL is only used for notifying the CCB of incidents. The information in the incident report form is secured during transit via encryption. If you prefer to send addtional sensitive information you can share with us via PGP encrypted mail. More info on how to do this can be found here: https://ccb.belgium.be/en/cert/send-encrypted-message
19	The report form is quite limited (some common characters are not allowed) and there is no way to see what has been sent, is there plan to change this ?	Thank you for your comment. It's useful to improve our reporting process.
20	The limitation of 500 characters and not being able to use attachments is also not very user friendly.	Thank you for your comment. It's useful to improve our reporting process.
21	I am being told that the captcha in use is also not user friendly.	Thank you for your comment. It's useful to improve our reporting process.
22	do we need to use a specific phone number to inform the police?	No there is no specific phone number. A cybersecurity crime can be reported (PV) to the local police.
23	currently there is no authentication towards notif.safeonweb.be . Are you going to adapt this ?	No, it will stay publically accessible without any authentication to avoid obstacle in the notification process. The URL is only used for notifying the CCB of incidents. We have protocols in place to verify the authenticity of incidents before deploying resources. Additionally, we continuously train our personnel to prioritize and manage incidents effectively, ensuring that genuine emergencies receive the attention they require. The information in the incident report form is secured during transit via encryption. If you prefer to send addtional sensitive information you can share with us via PGP encrypted mail. More info on how to do this can be found here: https://ccb.belgium.be/en/cert/send-encrypted-message
24	What steps should you take if you discover a data leak involving the personal contact information of a Belgian citizen, and the data was not lost by your own company? And is the CCB actively looking for these kind of attacks againt individuals, or only focusses on companies?	You can send the information to incidents@ccb.belgium.be. All kinds of notifications are processed by the CCB and if possible we do act on that information (i.e. informing the involved organizations or victims) The CCB focuses on any cyberincident involving Belgian organizations and citizens.
25	Will CCB act as CSIRT in all cases where help is requested (we don't all have a SOC / access to these capabilities))? Will CCB only recommend connecting with other authorities if help is requested?	The CCB will always provide a baseline level of assistance when we're notified of a cyber incident. Additionally, the CCB's Incident Response team could be deployed, upon your request, to provide a more hands-on approach to helping you out. The deployment of this team is decided on a case-by-case basis and depends on availability and other priorities. The CCB recommends contacting the police for any cyber incident with notable impact to availability, or financial damage. For a personal information data leak, the Data Protection Authority should be contacted. The CCB can recommend this in any case, even if you did not request help with the cyber incident you're experiencing.
26	What about multi-nationals with a significant presence in Belgium but main office abroad, do they need to report to CCB (and receive support) or does it need to go through the main office?	The NIS2 jurisdiction rules and the impact of the incident define where to notifiy the incident. See question 12.
27	Is there a link between the ticket for early notification and the 72h update? Do we have to refer to a ticket number for the 72h update?	You do not need to refer to the old notification. Our ticketing system will automatically receive your update and link it to your previous NIS2 notification.
28	Should an incident be reported in the country where it occurred or in the country where the headquarters is located?	The NIS2 jurisdiction rules and the impact of the incident define where to notifiy the incident. See question 12.

29	It would be useful if we could 'verify' that a company has reported compromised emails, so we can double-check in case of doubt	This is a good idea but not so useful if the company hasn't had the time to notify us, or if the company doesn't know yet that their e-mail is compromised. In case of doubt, we recommend that you contact the organization involved directly. Do not click on the links or call the number in the email, but contact the organization. If you do not have contact details yourself, you can use a search engine to look for contact details. They may or may not be able to confirm whether the message is genuine.
30	If the incident comes from a third party, and this third party is an essential organization (e.G. : electricity supplier), do we have to declare the incident ?	If you are a NIS2 entity and the incident qualifies as a "significant incident", you have an obligation to report this incident.
31	How aggressive is your monitoring? And are we informed beforehand our ranges are monitored - any sla?	In alignment with the NIS2 Directive, the CCB as the national CSIRT - is tasked with monitoring and analyzing cyberthreats, vulnerabilities and incidents at national level in order to provide warnings, notifications and announcements and disseminate information to Belgian constituents. The external scans are non-intrusive and help identify indicators of potentially high-risk major vulnerabilities and exposures known to be exploited by cyber criminals and/or nation-states (such as the Apache Log4j2 Remote Code Execution Vulnerability or an identified vulnerable version of a WordPress plugin that affects authentication). Thanks to these scans the CCB can inform the organization to help remediate the identified vulnerability. The list of assets scanned is limited to the IP addresses and ranges configured in the Early Warning System (EWS) portal.
32	Who is taking care of the out-border reporting? Do we need to report to other authorities or only local one ?	The NIS2 jurisdiction rules and the impact of the incident define where to notifiy the incident. See question 12.
33	What about incidents happening in Belgium, but the company is only a subsidiary of a company having HQ in another European country ? Should we report it in Belgium also or HQ reporting will be enough ? thanks	The NIS2 jurisdiction rules and the impact of the incident define where to notifiy the incident. See question 12.
34	Where can we find a list of organisations that fall under the NIS/2? Where can we find a list of obligations in this respect? Do we have an obligation towards NSA (NVO/ANS)? Do we need a security officer and security clearances for our field engineers?	The list of NIS2 entities is not publicly available (for security reasons). This information is only available for the CCB and the competent sectoral authorities.
35	When it comes to reporting to the police, do you mean for every single case of a significant incident or just when it comes to more physical incidents such as intruders on premises, stolen laptops, etc. ?	Cybercrime or regular crime (physical incidents) can be reported to the police. Reporting to the police is always a good idea in case of some kind of damage. This could be physical, financial or even virtual.
36	Is there any checklist available that help the relevant entities to assess if the incident is significant as it's not clear for some specific sector ?	You can find it here: https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20EN.pdf
37	NIS2 law in Belgium highlights that local public administrations such as municipalities and provinces aren't covered by the law, however they are still exposed to cyber threats and the supply chain as well makes them adopt several cybersecurity measures. How to make them understand that NIS2 is an opportunity for them and that they are concerned despite they think they aren't.	Local public administrations can be identified by the CCB and fall under the NIS2 law (there are plans to do so in the near future). Some local public administrations are falling under the NIS2 law when they provide a service covered in the annex of the NIS2 law. The CCB has issued a recommendation 1/2024 which encourages the implementation of CyFun for the public administrations in Belgium: https://ccbsite.prd.excom.fgov.be/sites/default/files/CCB%20richtlijn%20overheden%20v3%20FR.pdf https://ccbsite.prd.excom.fgov.be/sites/default/files/CCB%20richtlijn%20overheden%20v3%20NL.pdf

38	I needed to reported a recent incident to the local police department, and made an appointment to do so, at their office. During the interview, I had to explain to the police officer what a security incident was, what ransomware was, ... They did not have a clue what I was talking about. This took in total 2 hours and was a waste of time. Question: Can this police report be done online?"	We cannot comment on the Police's internal workings. To file an official report to the police it needs to happen at a local Police department . For non-urgent cases, an online report can be done, but this is not meant for cyber incidents. More information at: https://www.politie.be/police-on-web/nl
39	The Cybersecurity incident Management Guide link doesn't work: https://atwork.safeonweb.be/tools-resources/cyber-attacks-what-do?_x_zm_rtaid=tfJKWZrLSV6SBxVUV4yKvw.1739870532743.71edea67a5b3a8751880d999f01d4be6&_x_zm_rhtaid=550	We indeed saw that the link to the website of the Cyber Security Coalition is not working. We contacted them and they fixed the link.
40	How can I get the Cyfun label and who is handling the audit?	Go to https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework and download the CyberFundamentals Toolbox. 1. Perform a risk assesment to select your assurance level 2. Complete your Self-Assessment and implement corrective measures 3. Select an authorised Conformity Assessment Body and have them verify or certify your self-assessment 4. Request your label on the Safeonweb@work portal
41	Does the ccb have enough staff to handle all these reports. I can imagine there are a lot of reports coming in	The CCB is able to handle all incoming incident notifications and reports at the moment.
42	Significant incidents can also be non-cybersecurity related, don't these type of notifications risk to drown out the cybersecurity notifications?	See the notion of incident according the NIS2 law and directive (which includes cyberattacks but also technical failure, human errors, natural causes). Some incident reporting will not require direct actions from the CCB (statistical purposes).
43	where can we register for the next webinars ? The ones that Arnout mentionned that are taking places at the end of the month.	You can check and sign up for our future Connect and Share events here: https://events.zoom.us/eo/AhgwS4H5MFgNbmQvH-zQ9um2zt9wWmSQhfchj6xgmQmL-YVocY7h~AggLXsr32QYFjq8BlYLZ5I06Dg
44	Can we request CCB for performing a security audit of our organisation to obtain a Cyfun certificate?	No, to obtain a CyFun label (certification/verification), an audit must be carried out by an authorised Conformity Assessment Body (CAB). For their regular conformity assessment, essential NIS2 entities can choose from three options: 1. Certification/Verification: CyberFundamentals by an authorised CAB 2. Certification: ISO 27001 by an authorised CAB 3. Mandatory inspection by the CCB (with fees for the entity) The first two options give a presumption of conformity and a potential CyFun label. However, an inspection by the CCB will never lead to a CyFun label (certification/verification) or an ISO 27001 certification.
45	should we report incident like mail compromised but no impact on our daily business ?	Every significant incident should be reported. A compromised e-mail might not seem like much at first sight, but it could have severe impact later on. More information can be found in the incident notification guide here: https://ccb.belgium.be/sites/default/files/nis2/NIS2%20Notification%20guide%2010-2024%20v1.2%20-%20EN.pdf
46	is this webinar will be shared ?	Yes the recording will be shared as soon as possible with all registrants.
47	how much info will you share on lessons learned	We will regularly publish new tips and tricks and if required, we'll also adapt our guidelines.
48	Would you report statistics and analyis of incidents (and at what frequency)	The yearly report of statistics regarding incidents in 2024 will be published in the coming weeks. Thank you for your interest in this.
49	Practical question: will we receive the recording of this session? Cheers!	Yes the recording will be shared as soon as possible with all registrants.
50	Reference ticket number: all our requests go into Service NOW - automatic ticket number notification to the caller. Possible?	Thank you for the suggestions. Currently we have a system internally to easily refer to previous tickets without the caller/mailer having to provide us anything.