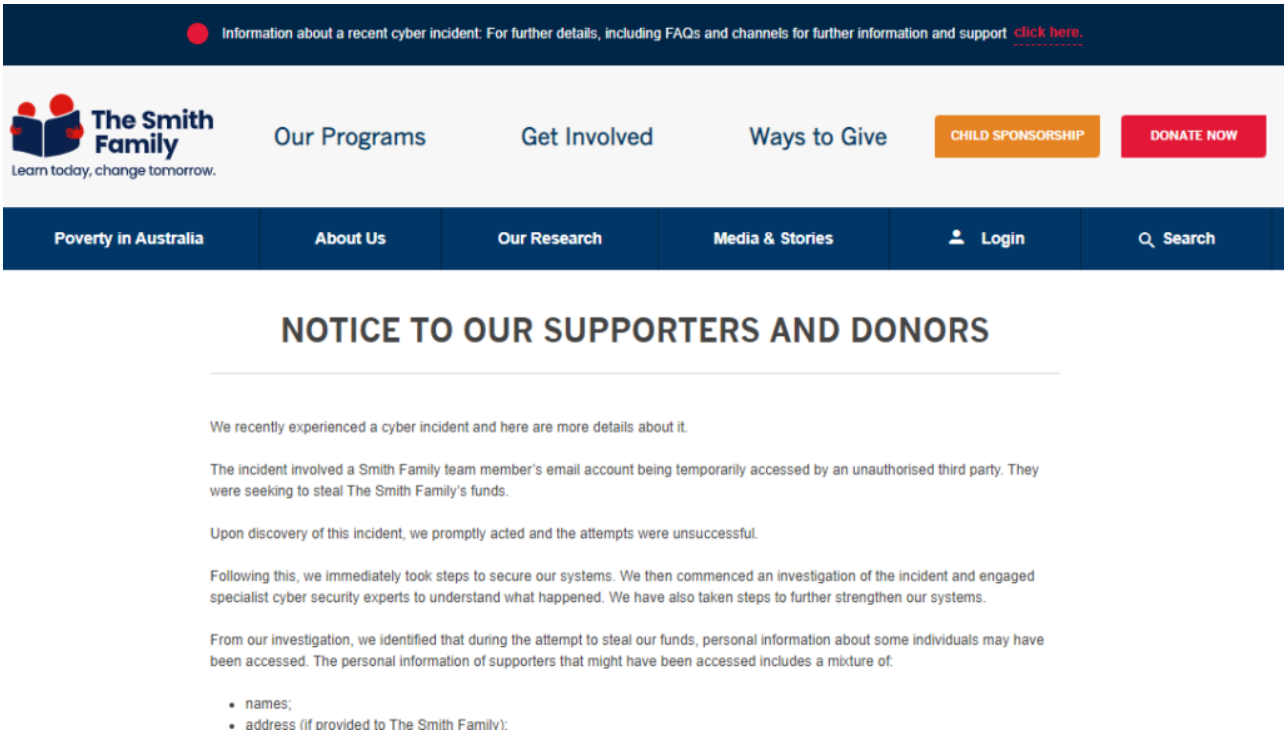
Comment réagir à un piratage de données – l'exemple de Smith Family

L'association australienne Smith Family (collecte annuelle environ 80M€) a été récemment victime d'une cyber attaque. Parallèlement aux actions techniques, sa réaction en termes de communication a consisté en la mise en avant sur son site d'une page dédiée explicative sur les circonstances de l'incident et ses conséquences pour les personnes concernées.



Une communication la plus transparente possible, organisée en 3 volets

Informer

NOTICE TO OUR SUPPORTERS AND DONORS

We recently experienced a cyber incident and here are more details about it.

The incident involved a Smith Family team member's email account being temporarily accessed by an unauthorised third party. They were seeking to steal The Smith Family's funds.

Upon discovery of this incident, we promptly acted and the attempts were unsuccessful.

Following this, we immediately took steps to secure our systems. We then commenced an investigation of the incident and engaged specialist cyber security experts to understand what happened. We have also taken steps to further strengthen our systems.

From our investigation, we identified that during the attempt to steal our funds, personal information about some individuals may have been accessed. The personal information of supporters that might have been accessed includes a mixture of:

- names;
- address (if provided to The Smith Family);
- phone number (if provided to The Smith Family);
- email address (if provided to The Smith Family); and
- donation amount.

And in some cases:

- first 4 and last 4 digits of the credit or debit card used to donate; and,
- information about whether a donation payment was processed successfully or declined

We can confirm for those with potential credit or debit card details accessed, no middle digits, or CVV numbers were accessed as The Smith Family does not store that information in its systems.

The data accessed in itself cannot be used to make fraudulent purchases.

Our investigation also identified some other information which may have been accessed but does not require formal notification.

The Smith Family also does not request, collect or hold personal identity documents such as passports or drivers' licences of our supporters, as these are not required to process their generous donations.

While there is no current evidence of misuse of any individual's personal information, we are informing individuals about the incident and providing simple steps to protect their information and avoid any potential scams.

We are also contacting individuals whose personal information was not accessed and are not directly affected by this incident as we want to communicate transparently to our supporters.

- Cet incident a-t-il un rapport avec le vol de données Medibank ?
- Les autorités ont-elles été informées ?
- Comment puis-je savoir que cette affaire sera terminée pour ce qui me concerne ?

Expliquer

- Comment nous-sommes-nous rendu compte de l'incident
- Comment le pirate a-t-il pu accéder à l'email de notre collaborateur
- Pourquoi Smith Family dispose-t-elle d'informations personnelles à mon sujet ?

Rassurer

- L'attaque a-t-elle été interrompue

- Des données personnelles ont-elles été divulguées
- Comment savez-vous qu'aucune donnée personnelle n'a été utilisée
- Nos systèmes sont-ils toujours opérationnels ?
- Dois-je annuler ma carte bancaire ?
- Que dois-je faire maintenant ?
- Puis-je toujours faire un don en ligne ?

Pour information, l'association semble utiliser la solution CRM Dynamics 365. *voir ici*

Mon assoc est-elle data-driven ? 2/2 – l'opérationnel

Suite de notre précédent post (voir ici)

Des questions plus opérationnelles, comme chacun sait le diable se niche dans les détails

	Les données sont utiles. Que ce soit à l'occasion d'une migration, ou lors de la mise en place de nouveaux process, il est bon de se poser la question de la légitimité à conserver et utiliser telle ou telle donnée. Inutile de s'encombrer !
	Les données sont uniques. L'adresse d'un contact, par exemple, est enregistrée dans une table et une seule. Si cela n'était pas possible des synchronisations sont mises en œuvre pour éviter toute incohérence.

	les données sont de bonne qualité Les adresses sont au format postal, des référentiels communs aux différents outils ont été définis (projets, thématiques d'engagement, etc.), des traitements sont régulièrement exécutés pour identifier les problèmes et les résoudre automatiquement dans la mesure du possible.
	les données sont fraîches, et leur mise à jour est fluide et robuste Les mises à jour sont effectuées en temps réel. Un historique des modifications effectuées peut être activé si besoin. Les traitements automatiques et notamment ceux concernant l'intégration de flux externes sont effectués au fil de l'eau, et ne compromettent pas l'intégrité des données.

Mon assoc est-elle data-driven ? 1/2 – la stratégie

Comment piloter mon association par les données ? (est-elle "data-driven")
Une question toujours plus d'actualité, à l'heure du marketing digital et de l'interopérabilité des systèmes d'information.
quelques questions à se poser, pour faire le point et identifier des axes d'amélioration.

Dans un second post, j'évoquerai quelques aspects plus opérationnels.

	**Une politique de la donnée est définie et suivie** Une instance en lien avec la gouvernance regroupe stratèges, utilisateurs métiers, techniciens de la donnée.
	**Les données sont enregistrées dans des bases de données structurées** Un dictionnaire des données existe et est régulièrement mis à jour. L'architecture des données est connue. Des référentiels communs aux différents outils métiers peuvent être utilisés.
	**Les données sont exploitables par des outils d'analyse** Un modèle de données est défini afin de permettre aux utilisateurs métiers de disposer et éventuellement de concevoir des tableaux de bord de suivi et de pilotage de leur activité.
	**Les données personnelles sont hébergées de façon sécurisée et conformément au RGPD** De nombreux sujets doivent être réglés, tels que la sécurité de l'hébergement (plan de reprise d'activité, disponibilité), ainsi que sa localisation (UE), le consentement des contacts, la protection des accès, l'identification des prestataires, la justification des traitements, etc. La mise en conformité RGPD est d'ailleurs un bon moyen de rentrer dans une démarche "data-driven".
	**Les données peuvent être partagées et sont accessibles selon l'usage** Des règles sont définies pour permettre à chaque utilisateur autorisé un accès contrôlé aux données.

Se préparer à un contrôle de la CNIL

la CNIL vient de mettre en ligne une charte des contrôles dans laquelle vous trouverez un grand nombre d'informations utiles.

le document complet peut être téléchargé sur le site de la CNIL en cliquant ici

1. Les caractéristiques d'un contrôle

Objectifs

	S'assurer que le traitement ne porte pas atteinte aux droits et libertés des personnes S'assurer que les organismes répondent au principe de responsabilisationla CNIL s'intéressera notamment • à la finalité du traitement • à la nature des données collectées • aux modalités d'information des personnes • aux durées de conservation • aux destinataires des données personnelles • aux moyens de sécurité mis en oeuvre • aux transferts des données personnes le cas échéant

Qui peut être contrôlé ?

	Tout organisme traitant des données personnelles Ses prestataires sous-traitants (hébergement, maintenance, etc.)

Comment la CNIL décide-t-elle de procéder à un contrôle ?

	Selon ses thématiques annuelles de contrôle (en 2020 : données de santé, géolocalisation, cookies) Suite à une réclamation ou une plainte A son initiative Les dispositifs de vidéoprotection A la suite d’une procédure de contrôle clôturée

Quelles sont les différentes formes de contrôle ?

	Contrôle sur place Contrôle sur convocation Contrôle en ligne Contrôle sur pièces

2. Les pouvoirs des agents de contrôle

Pouvoir d’accès aux locaux

	Accès entre 6h et 21h

Pouvoir de se faire communiquer tous renseignements ou documents utiles

Obligations des agents de contrôle

	Secret professionnel Ils ne peuvent participer au contrôle d’un organisme dès lors qu’ils y ont détenu un intérêt direct ou indirect dans les 3 années précédent le contrôle, qu’ils y exercent ou y ont exercé une activité professionnelle, qu’ils détiennent ou ont détenu un mandat.

3. Les droits des organismes contrôlés

Identité des contrôleurs et information sur l’objet du contrôle

Peut-on refuser le contrôle de la CNIL ?

	Cela n’est pas possible

Peut-on opposer le secret professionnel ?

	Dans certains cas : relation avocat/client, sources journalistiques, secret médical. Concernant le secret médical, celui-ci ne peut être opposé si un médecin accompagne la délégation de la CNIL.

Peut-on se faire assister d’un conseil ?

	Oui

4. Le déroulement d’un contrôle

Contrôle sur place

	Avant le début de la mission, les agents de contrôle demandent à être mis en relation avec le représentant légal, un responsable en lien avec le traitement, ou encore toute personne exerçant une activité professionnelle au sein de l’organisme. Cet interlocuteur devra se rendre disponible pour suivre les agents tout au long du contrôle, et relire et signer le procès-verbal. Des entretiens sont menés, et des pièces recueillies. Un procès verbal est dressé, soumis à relecture et signature.

Contrôle en ligne

	Les agents accèdent aux sites de l’organisme depuis les locaux de la CNIL. Ils se comportent comme tout internaute, peuvent compléter des formulaires en ligne, tester des liens de désincription ou des procédures permettant l’exercice de leurs droits. Un procès verbal est dressé, qui peut faire mention de demande de communications de pièces complémentaires (contrats, extractions de base de données, etc.)

Contrôle sur audition

	Un courrier de convocation est adressé à l’organisme au moins 8 jours avant la date de l’audition. Le déroulement est similaire au contrôle sur place (entretiens, recueil de pièces, procès verbal).

Contrôle sur pièces

	Un questionnaire est envoyé par la CNIL, destiné à recueillir des éléments d'information ainsi que des pièces et documents justificatifs. La réponse peut être faite au format papier ou numérique (envoi d'un email, support numérique).

5. les suites d'un contrôle

Notification du procès verbal

	Dans un délai de 15 jours à compter du contrôle.

Instruction du dossier

	Des demandes complémentaires peuvent être adressées à l'organisme. Elle peut se dérouler sur une période de plusieurs mois.

Suites possibles

	Clôture de la procédure avec ou sans observations Avertissement et rappel à l'ordre par la Présidente de la CNIL Mise en demeure Décisions prononcées par la formation restreinte pouvant prononcer des sanctions ou une relance : • rappel à l'ordre ; • injonction de mettre le traitement en conformité ; • limitation temporaire ou définitive du traitement ; • retrait d'une certification ; • suspension de flux de données ; • amende administrative.

RGPD : la réaction de Save

the Children face à une violation de données

Comment réagir si votre base de données est piratée d'une façon ou d'une autre , et que cette violation concerne des données personnelles ou sensibles ?

Au delà des réponses techniques, la communication auprès des personnes concernées est un sujet important. La CNIL précise les actions à mener en cas de violation des données personnelles (Voir ici sur le site de la CNIL) :

- Documenter les incidents ;
- Informer la CNIL ;
- Dans certains cas, informer les personnes concernées.

L'exemple récent (mai – juillet 2020) de l'ONG Save the Children est un cas d'école

Les parties prenantes

- l'ONG américaineSave the Children ;
- Blackbaud, éditeur et hébergeur de la base de données.

L'incident

En mai 2020 Blackbaud est victime d'une attaque de type « ransomware » : Un hacker s'introduit sur un serveur hébergeant des données pour en perturber le fonctionnement ou le bloquer jusqu'à paiement d'une rançon.

- Interruption du service ;
- Cryptage des données ;
- Vol de données.

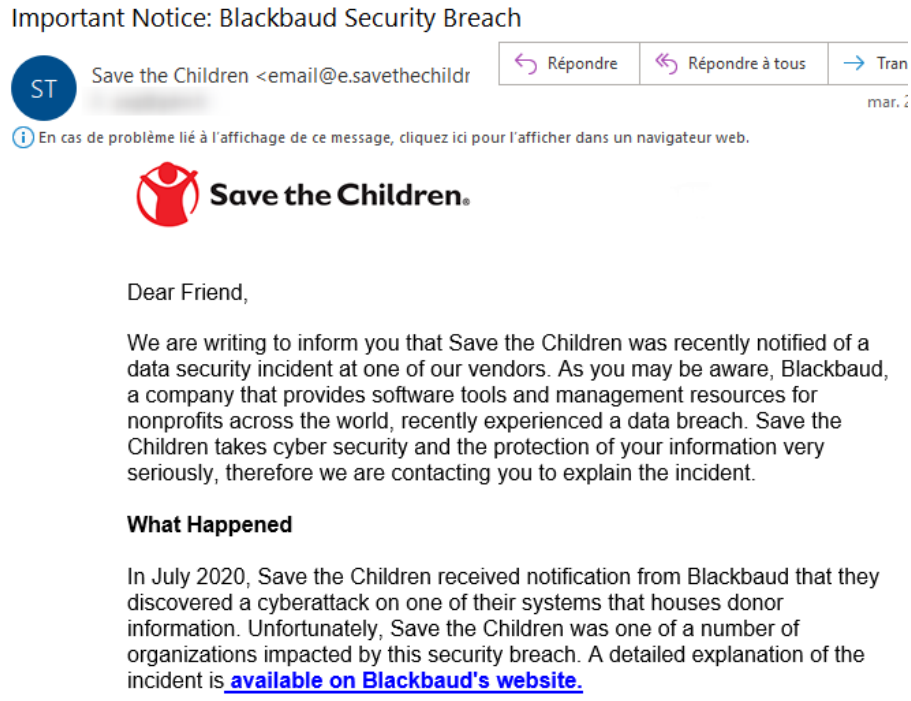
Blackbaud a payé la rançon, et s'est assuré que les données dérobées ont bien été détruites (le hacker étant supposé être une personne de confiance !)

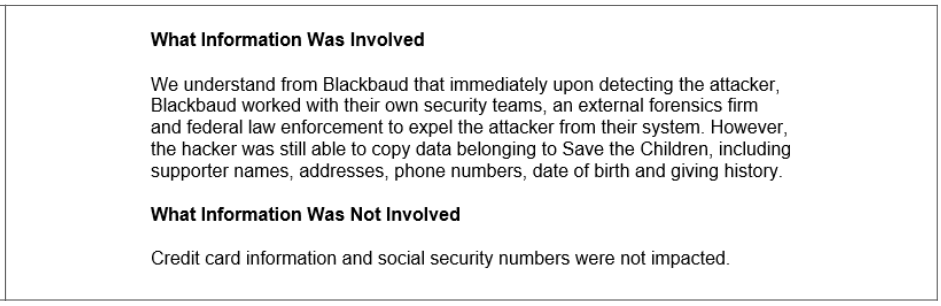
La communication de l’ONG

- juillet 2020 : envoi d’un email aux contacts (donateurs ou non)
- Information sur le site (voir ici)

Une information a également été faite sur le site de l’éditeur Blackbaud (voir là).

Le détail de l’email d’information

Le contexte, la présentation des parties prenantes	

Le détail de l’incident, et les données concernées	

Les mesures prises par Blackbaud • Paiement de la rançon ! • Mise en place d’une surveillance accrue Les mesures prises par l’ONG • Changement d’hébergeur	**Blackbaud's Response** Blackbaud obtained confirmation that the data was deleted in exchange for a payment to the hacker, and has provided assurances to Save the Children that the risk to individuals whose data was stolen is very low. In an abundance of caution, Blackbaud has put in place dark web monitoring intended to detect trafficking of any of the copied data, and Save the Children will maintain regular contact with Blackbaud to stay well informed of any developments of this nature. **Save the Children's Response** Save the Children places the highest level of regard on security and protecting our donor information. We have removed our data off Blackbaud's servers, and will continue to prioritize security, both internally and with all of our third-party vendors. Supporters like you trust us with their information, and we do not take this lightly. We have and will continue to take steps to protect supporters' information in our combined efforts to ensure every child gets the future they deserve. Save the Children remains in regular contact with Blackbaud regarding any further details of this incident, and we are continuing to monitor their response. If you have any immediate concerns or questions, please contact our Supporter Experience Center at 1-800-728-3843.