OCHA centre for humdata

مركز البيانات الإنسانية

سلسلة المذكرات الإرشادية

مسؤولية البيانات في العمل الإنساني

إدارة حوادث البيانات

النقاط الرئيسية:

- حوادث البيانات الإنسانية هي أحداث تتعلق بإدارة البيانات وقد تسببت في ضرر أولديها القدرة على التسبب في ضرر للأشخاص المتأثرين بالأزمات، والمنظمات وعملياتها، والأفراد أو المجموعات الأخرى.
- تشمل أمثلة حوادث البيانات الإنسانية الاختراقات الفيزيائية للبنية التحتية، الكشف غير المصرح به للبيانات، واستخدام بيانات المستفيدين لأغراض غير إنسانية، من بين أمور أخرى.
- لحادث البيانات أربعة جوانب: ١) مصدر التهديد، (٢) حدث التهديد، (٣) الضعف٤التأثير السلب.
- هناك خمس خطوات للاستجابة لحوادث البيانات: (١) الإخطار، (٢) التصنيف، (٣) المعالجة، و (٤) إغلاق الحادث، بالإضافة إلى (٥) التعلم.

ما هو حادث البيانات في الاستجابة الإنسانية؟

في القطاع الإنساني، حوادث البيانات هي أحداث تتعلق بإدارة البيانات التي تسببت في ضرر أو لديها احتمالية التسبب في ضرر للسكان المتأثرين بالأزمات، والمنظمات الإنسانية وعملياتها، والأفراد أو المجموعات الأخرى. يمكن لهذه الأحداث أن تستغل أو تزيد من نقاط الضعف الموجودة.[١] في بعض الحالات، قد تخلق أيضًا نقاط ضعف جديدة يمكن أن تزيد من خطر حدوث حوادث بيانات في المستقبل.

لم يكن لدى العاملين في المجال الإنساني فهم مشترك لما يشكل حادث بيانات، ولا يوجد معيار تقني أدنى لكيفية منع هذه الحوادث وإدارتها. سيلعب تطوير القطاع الإنساني للأدوات وتنفيذ الإجراءات لإدارة حوادث البيانات دورًا مهمًا في تطور المعايير الأخلاقية وحقوق الإنسان والتقنية والمهنية للعمليات الإنسانية.»

> «إذا قام العاملون في مجال المساعدات برقمنة المزيد من بياناتهم واتصالاتهم، فإنهم بحاجة ماسة إلى زيادة جهودهم في الأمن الرقمي. على الرغم من أن بعض الجهات الفاعلة تطور أدوات حماية واعدة، فقد يكون من الجيد للمنظمات الإنسانية بشكل عام أن تستمع إلى اقتباس من دوائر الأمن التقني: ‹هناك نوعان من المنظمات: تلك التي تم اختراقها، وتلك التي سيتم اختراقها.›»
>
> - راحيل ديت، «لا ضرر رقمي: التخفيف من مخاطر التكنولوجيا في السياقات الإنسانية»

قد تشمل حوادث البيانات الإنسانية اختراقات فيزيائية للبنية التحتية، والكشف غير المصرح به للبيانات، واستخدام بيانات المستفيدين «المجهولة» لأغراض غير إنسانية، من بين أمور أخرى. يمكن أن تحدث حوادث البيانات أيضًا دون أن يتم اختراق البنية التحتية التقنية بأي شكل من الأشكال. يمكن أن يكون لجمع البيانات واستخدامها ومشاركتها بشكل مشروع من قبل العاملين في المجال الإنساني آثار تشغيلية قد تشكل حادث بيانات في الحالات التي تؤدي فيها الشائعات، والحساسيات الثقافية، والديناميكيات السياسية، وعوامل أخرى إلى تأثيرات سلبية مرتبطة بالبيانات.

[١] «الضعف هو نقطة ضعف في نظام المعلومات أو إجراءات أمن النظام أو الضوابط الداخلية أو التنفيذ يمكن أن يستغلها مصدر التهديد.» منشور خاص من NIST ٨٠٠-٣٠ الإصدار ١، دليل لإجراء تقييمات المخاطر.

التعريفات وأطر الاعمال لفهم حوادث البيانات

طورت الحكومات والقطاع الخاص تعريفات وأطر عمل لفهم حوادث البيانات التي تعمل كمرجع مفيد للقطاع الإنساني.

- تُعرّف المنظمة الدولية للتوحيد القياسي (ISO) في معيار ISO ٢٧٠٠٠ «الحادث الحرج» بأنه «حدث واحد أو سلسلة من أحداث أمن المعلومات غير المرغوبة أو غير المتوقعة التي لديها احتمال كبير بتعريض عمليات الأعمال للخطر وتهديد أمن المعلومات.»[٢]

- يُعرّف المعهد الوطني للمعايير والتكنولوجيا (NIST) التابع لوزارة التجارة الأمريكية حدثًا ضارًا يتضمن «تهديدًا سيبرانيًا» بأنه «[حدث أو حالة لديها القدرة على التسبب في فقدان الأصول والعواقب غير المرغوبة أو التأثير الناتج عن هذا الفقدان.»[٣]

- يُحدد محمود شير-جان من الرابطة الدولية لمحترفي الخصوصية (IAPP) ثلاث فئات إضافية من الأحداث التي توسع تعريف NIST للأحداث الضارة. هذه الفئات هي، بترتيب تصاعد الخطورة: حوادث الأمان؛ حوادث الخصوصية؛ وانتهكات البيانات.[٤]

أمثلة على حوادث البيانات الإنسانية المحتملة

يتضمن حادث البيانات أربعة عوامل: مصدر التهديد، حدث التهديد، الضعف، والتأثير السلبي .[٥]

يما يلي نوعان من الحوادث الافتراضية التي قد تحدث في السياقات الإنسانية.

السيناريو الأول هو حادث اختراق بيانات نموذجي في سياق نزاع مسلح. والثاني هو مثال على نوع الثغرات التي يمكن أن تؤدي إلى حوادث بيانات فريدة من نوعها في القطاع الإنساني

١. يحدث الوصول غير المصرح به إلى البيانات [**التأثير**] بسبب مهاجمة جهات مسلحة [**المصدر**] لمرفق والاستيلاء على محركات الأقراص الصلبة التي تحتوي على بيانات المستفيدين [**الحدث**]. كانت محركات الأقراص غير مشفرة [**الضعف**].

٢. يؤدي غياب التوجيهات الي تحد من جمع البيانات لغرض معين [**الضعف**] إلى قيام الموظفين بجمع بيانات عن الحالة الزوجية للنساء الحوامل [**المصدر**]. يحدث اختراق للبيانات [**الحدث**] فيما بعد، مما يؤدي إلى زيادة فرصة العنف الجسدي [**التأثير**] ضد المستفيدات الحوامل غير المتزوجات.

توضح هذه السيناريوهات كيفية التفكير في تحديد سلاسل السببية التي قد تخلق حوادث بيانات محددة للسياق.

[2] International Organization for Standardization, ISO/IEC 27000:2018.

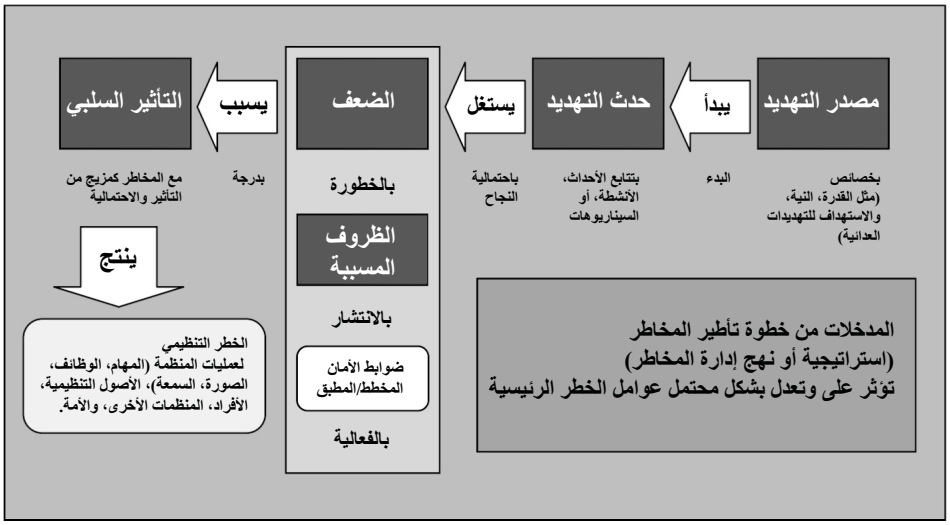
[3] NIST Computer Security Resource Center Glossary.

[4] IAPP, Is It an Incident or a Breach, How to Tell and Why It Matters, Mahmoud Sher-Jan (February 2017).

[5] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

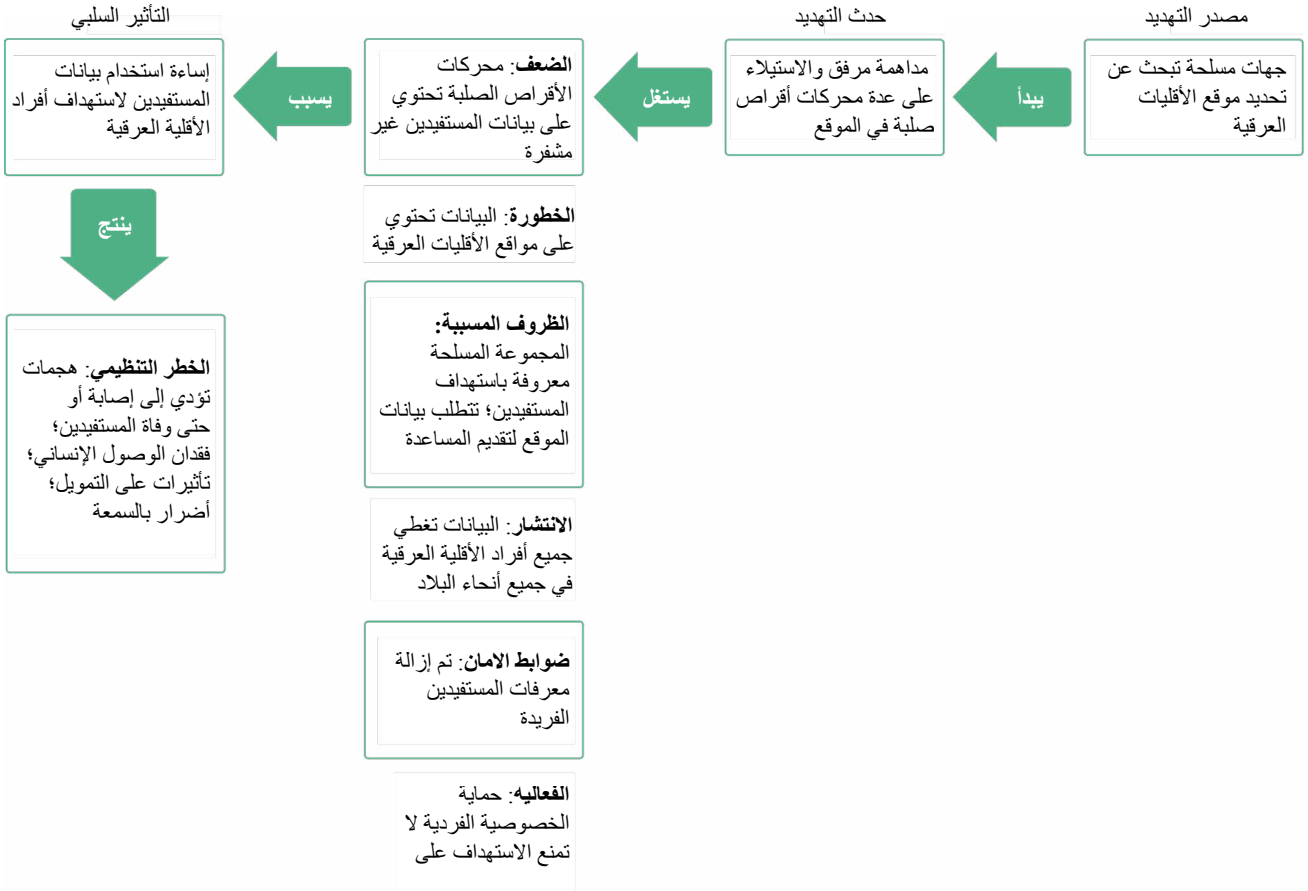
نماذج المخاطر

يوضح الشكل أدناه نموذج مخاطر عام مع عوامل الخطر التي يمكن للمنظمات استخدامها لفهم كيفية حدوث حادث بيانات. يستغل حدث التهديد ثغرة موجودة يتم تضخيمها بواسطة الظروف المسببة أو يتم التخفيف منها بواسطة ضوابط الأمان الموجودة بالفعل. يتسبب هذا في تأثيرات سلبية تنتج عن مخاطر تنظيمية، والتي يمكن أن تشمل المخاطر على المنظمة وعلى الأشخاص المتأثرين.



[6] الشكل ١. «نموذج المخاطر العام مع عوامل الخطر الرئيسية». المصدر: منشور خاص من NIST ٨٠٠-٣٠ الصفحة ١٢

يقدم الشكل أدناه مثالاً على كيفية تعديل هذا النموذج العام للمخاطر ليتناسب مع القطاع الإنساني.



الشكل ٢. نموذج المخاطر مع عوامل الخطر الرئيسية المعدلة لتناسب السياق الإنساني.

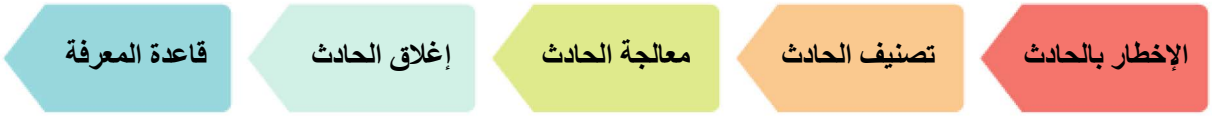
[6] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.

يمكن للمنظمات الإنسانية تطوير نماذج مخاطر خاصة بها لإدارة حوادث البيانات تتضمن هذه العوامل. ستختلف طبيعة عوامل الخطر هذه مجتمعة معا لتشكيل حادث بيانات من منظمة إلى أخرى ويجب تكييفها مع الواقع التشغيلي المحدد.

خطوات إدارة حوادث البيانات

بعد تعريف واضح لما يشكل حادث بيانات، يمكن للمنظمات تطوير إجراءات تشغيل قياسية (SOPs) لإدارة حوادث البيانات.

يجب أن تتضمن SOPs لإدارة حوادث البيانات الخطوات الخمس التالية: ١) الإخطار، ٢) التصنيف، ٣) المعالجة، ٤) الإغلاق، و ٥) قاعدة المعرفة.[٧]



الشكل ٣: خمس خطوات في معالجة حوادث الأمان (المصدر: كيفية التعامل مع الحوادث وفقًا لـ ISO ٢٧٠٠١ A.١٦، أنطونيو خوسيه سيغوفيا).[٨]

يمكن أن تبدو تطبيقات هذه الخطوات في منظمة ما على النحو التالي:

١. الإخطار بالحادث: يكشف شخص حادثة ويبلغ الزملاء المناسبين وفقًا لإجراءات الاتصال في المنظمة (عادةً عبر البريد الإلكتروني أو مكالمة هاتفية أو أداة برمجية، إلخ). يجب أن يحتوي الإخطار، إن أمكن، على وصف للعوامل الرئيسية للمخاطر المتضمنة في الحادث: المصدر، الحدث، الضعف والتأثير.

٢. تصنيف الحادث: يصنف متلقي الإخطار الحادث بناءً على تأثيره (عالي، متوسط أو منخفض)[٩] ومدى الحاجة إلى المعالجة (عالي، متوسط أو منخفض). تبدأ إدارة المخاطر بتصنيف جميع الحوادث، سواء نتج عنها ضرر ملموس أم لا.[١٠]

٣. معالجة الحادث: يقرر خبير تقني التدابير اللازمة لمعالجة الحادث بمجرد تصنيف الحادث والاتفاق على الوقت المخصص للمعالجة.

٤. إغلاق الحادث: يتم تسجيل جميع المعلومات التي تم توليدها خلال المعالجة ويتم إبلاغ الشخص الذي أرسل الإخطار الأولي أن الحادث قد تم إغلاقه.

٥. قاعدة المعرفة: تُستخدم جميع المعلومات التي تم توليدها خلال معالجة الحادث لإبلاغ وتدريب الزملاء وكمواد مرجعية للحوادث المشابهة في المستقبل.

يمكن للمنظمات الإنسانية أن تبني إجراءات التشغيل القياسية الخاصة بها على هذا النموذج المكون من الخطوات الخمسة، موضحة كيفية تنفيذ كل خطوة داخل المنظمة. يجب أن يتضمن ذلك الوظائف/الأدوار والفرق داخل المنظمة المسؤولة في كل مرحلة من العملية. يجب دمج هذه الخطوات في بروتوكولات الاستجابة للحوادث الموجودة أو توسيعها (مثل إدارة حوادث الأمن المتعلقة بالوصول الإنساني).

في سياق استجابة معينة، يجب على المنظمات العمل على دمج أي إجراءات مشتركة لإدارة الحوادث في هياكل التنسيق الحالية، مثل المجموعات والآليات للتنسيق بين المجموعات وداخلها.

[7] The Centre for Humanitarian Data provides several sources of guidance that can inform the development of Data Incident Management SOPs on the **Data Responsibility page**.

[8] **How to handle incidents according to ISO 27001 A.16**, Antonio Jose Segovia, (October 2015.).

[9] For humanitarian organizations, an example of such a classification is the World Health Organization's (WHO) **International Classification of Patient Safety, Conceptual Framework for the International Classification of Patient Safety**.

[10] WHO, **Conceptual Framework for the International Classification of Patient Safety**.

التوصيات لتحسين إدارة حوادث البيانات في المنظمات الإنسانية

ان تقديم أو تحسين إدارة حوادث البيانات في العمليات الإنسانية أمرًا في غاية الاهمية لممارسة البيانات بشكل أكثر مسؤولية في القطاع. يوصي مركز البيانات الإنسانية بأن تركز المنظمات على المجالات التالية:

١. تأسيس فهم مشترك لإدارة حوادث البيانات
استخدم نموذج مخاطر لفهم سلسلة السببية التي يمكن أن تؤدي إلى حوادث البيانات لمكاتب وأنظمة معينة. حدد الجهات الفاعلة الرئيسية للتهديد ونقاط الضعف للمكاتب والأنظمة وفهم ضوابط الأمان الموجودة وفعاليتها. أخيرًا، قم بتحديد القدرة الحالية لإدارة حوادث البيانات وتحديد ما إذا كانت في المكان المناسب. بمجرد تحديد التعريفات والعمليات بشكل واضح، استثمر في زيادة وعي الموظفين ودعم ثقافة الحوار المفتوح حول الحوادث، حيث يتم تحفيز الإبلاغ الاستباقي وإدارة الحوادث بدلاً من معاقبتها.

٢. تعزيز قدرة إدارة حوادث البيانات
اتخذ تدابير لوضع ضوابط أمنية لتقليل خطر حوادث البيانات، وشارك أفضل الممارسات مع الشركاء. قم بالبناء على العمل الحالي في القطاع لسد فجوات الحوكمة التي يمكن أن تخلق نقاط ضعف لمنظمتك. تفاعل مع شركاء المنظمة لإنشاء قنوات للمعلومات حول حوادث البيانات. شارك نقاط الضعف المعروفة بطريقة محكومة مع نظراء موثوق بهم للتعلم المتبادل بين المنظمات.

٣. دعم التعلم المستمر
ادعم التعلم وتطوير ممارسات محسنة لإدارة حوادث البيانات من خلال تنظيم تدريبات ومناورات بناءً على السيناريوهات المحتملة في البيئات التشغيلية المختلفة. يجب أن تحدث هذه التدريبات بانتظام وقد تشمل حتى تدريب ومناورة منظمات متعددة معًا. بالإضافة إلى ذلك، وثق حوادث البيانات الفعلية كحالات لتطوير المعرفة الداخلية.

تشجع المنظمات على مشاركة تجربتها في تطوير إدارة حوادث البيانات مع مركز البيانات الإنسانية عبر البريد الإلكتروني:centrehumdata@un.org.

المتعاونون: جامعة ييل، معهد جاكسون للشؤون العالمية.

ينشر مركز البيانات الإنسانية («المركز»)، بالتعاون مع الشركاء الرئيسيين، سلسلة من ثماني مذكرات إرشادية حول مسؤولية البيانات في العمل الإنساني خلال عامي ٢٠١٩ و٢٠٢٠. تتبع سلسلة المذكرات الإرشادية نشر إرشادات مسؤولية البيانات لمكتب تنسيق الشؤون الإنسانية في مارس ٢٠١٩. من خلال هذه السلسلة، يهدف المركز إلى تقديم إرشادات إضافية حول القضايا والعمليات والأدوات المحددة لمسؤولية البيانات في الممارسة العملية. تم تمكين هذه السلسلة بفضل الدعم السخي من المديرية العامة للحماية المدنية وعمليات المساعدة الإنسانية الأوروبية (DG ECHO).

يغطي هذا المستند أنشطة المساعدات الإنسانية المنفذة بمساعدة مالية من الاتحاد الأوروبي. لا ينبغي بأي شكل من الأشكال اعتبار الآراء الواردة هنا تعبيرًا عن الرأي الرسمي للاتحاد الأوروبي، كما أن المفوضية الأوروبية ليست مسؤولة عن أي استخدام قد يتم للمعلومات التي يحتويها.

هذا المشروع ممول جزئيًا
من الاتحاد الأوروبي