

إدارة الأزمات

د. آية عياد

PRL 631
برنامج ماجستير العلاقات العامة

المحاضرة العاشرة



إدارة الأزمات

المحاضرة العاشرة

PRL 631

برنامج ماجستير العلاقات العامة

إعداد:
د. آية عياد

إدارة الأزمات في عصر الرقمنة والذكاء الاصطناعي

مرحبًا بكم في المحاضرة العاشرة من مقرر "إدارة الأزمات"

- استعرضنا في المحاضرة التاسعة موضوع قياس وتقييم الأداء والتعلم من الأزمات، بدءًا من أهمية التقييم والقياس في إدارة الأزمات، وآليات تحديد مؤشرات الأداء الرئيسية KPIs لحملات العلاقات العامة في الأزمات، وطرق تقييم فعالية إدارة الأزمات في العلاقات العامة، إلى استخدام البيانات والتحليلات لتوجيه استراتيجيات إدارة الأزمات في العلاقات العامة
- ونتناول في المحاضرة العاشرة موضوع إدارة الأزمات في عصر الرقمنة والذكاء الاصطناعي، بدءًا من فهم الأزمات الرقمية، ودور الذكاء الاصطناعي في إدارة الأزمات، والتحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات، واستراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات، إلى دراسة حالة: إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي.

A COMPLETE GUIDE TO CRISIS MANAGEMENT



إدارة الأزمات في عصر الرقمنة والذكاء الاصطناعي

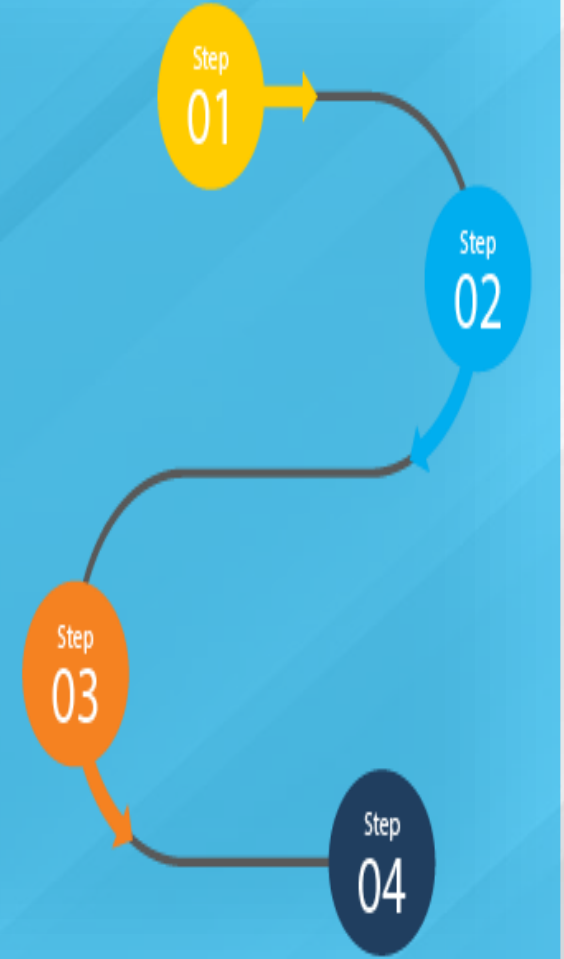
أولاً: الأزمات الرقمية

ثانياً: دور الذكاء الاصطناعي في إدارة الأزمات

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

رابعاً: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

خامساً: دراسة حالة: إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي



أولاً: الأزمات الرقمية

1. تعريف الأزمات الرقمية

. الأزمات الرقمية هي تلك الأزمات التي تنشأ نتيجة لمشاكل تقنية وأحداث مرتبطة بالرقمنة من خلل أو هجوم أو فشل تقني يؤدي إلى تعطل الأنظمة الإلكترونية، تسريب بيانات، أو إيقاف الخدمات.

. الأزمات الرقمية لم تعد تقتصر على الأعطال أو الاختراقات التقنية، بل تشمل أيضاً الأزمات الناشئة عن البيئة الرقمية والمعلوماتية مثل:

- . حملات التضليل المنسقة
- . التزييف العميق (Deepfake)
- . تسريب/إساءة استخدام المحتوى المولد بالذكاء الاصطناعي
- . الهجمات على السمعة الرقمية
- . الأزمات الناتجة عن أخطاء أنظمة الذكاء الاصطناعي

أولاً: الأزمات الرقمية

2. أنواع الأزمات الرقمية:

- **اختراقات البيانات Data Breaches:** حدوث تسريب أو سرقة للبيانات الحساسة من نظم المعلومات في المؤسسة.
- **الهجمات الإلكترونية Cyber Attacks:** تشمل هجمات الفدية، والبرامج الخبيثة، وهجمات DDoS التي تهدف إلى تعطيل الخدمات الإلكترونية.
- **الأعطال التقنية Technical Failures:** انقطاع الأنظمة أو فشل في البنية التحتية التقنية التي تدعم العمليات اليومية للمؤسسة.
- **فقدان البيانات Data Loss:** فقدان البيانات بسبب عطل في النظام أو خطأ بشري، والذي يمكن أن يكون له تأثيرات سلبية على استمرارية العمل.
- **أزمات التضليل الرقمي والمعلومات المضللة (Disinformation Crises)**
- **أزمات التزييف العميق وانتحال الهوية الرقمية (Deepfake & Synthetic Identity Crises)**
- **أزمات أخطاء الذكاء الاصطناعي المؤسسي (AI Failure Crises)**

أولاً: الأزمات الرقمية

2. أنواع الأزمات الرقمية:

النوع	الشرح المختصر	مثال من الواقع
اختراق البيانات	وصول غير قانوني لمعلومات حساسة	تسريب بيانات بطاقات العملاء لدى BankFirst في الإمارات 2024
هجمات إلكترونية	إيقاف خدمات أو ابتزاز مالي	هجوم فدية على مستشفى السلطان قابوس في عُمان 2024
أعطال تقنية	خلل في الأنظمة يؤدي لتعطيل العمليات	توقف خدمات Flynas في السعودية بعد خلل في نظام الحجز 2025
فقدان البيانات	ضياع ملفات مهمة	تعطل خادم بلدية الإسكندرية 2024 بسبب حريق أدى لفقد سجلات رقمية

أولاً: الأزمات الرقمية

3. الاختلافات بين الأزمات الرقمية والأزمات التقليدية:

- **سرعة الانتشار:** الأزمات الرقمية تنتشر بسرعة كبيرة، خاصة إذا تم استغلال وسائل التواصل الاجتماعي لنشر المعلومات، مما يجعل السيطرة عليها أكثر تحديًا.
- **تأثيرها على الأعمال:** الأزمات الرقمية يمكن أن تؤدي إلى خسائر مالية كبيرة، تقويض الثقة مع العملاء، وتعرض المؤسسة للمساءلة القانونية.
- **البنية التحتية التقنية:** تتطلب الأزمات الرقمية استجابة تقنية محددة مثل استعادة البيانات، تعزيز الأمن السيبراني، أو إصلاح الأنظمة المعطلة.

أولاً: الأزمات الرقمية

3. الاختلافات بين الأزمات الرقمية والأزمات التقليدية:

العنصر	الشرح	مثال
سرعة الانتشار	تنتشر عبر الإنترنت فوراً	شائعة إغلاق بنك خليجي خلال دقيقة عبر TikTok 2024
تأثير مالي سريع	الخسارة تحدث لحظياً	خسائر منصة Binance بملايين خلال نقاط اختراق متتالية 2024
مسؤوليات قانونية	لوائح حماية بيانات صارمة	غرامة على شركة اتصالات عربية لعدم حماية بيانات المشتركين 2024

أولاً: الأزمات الرقمية

4. تأثير الأزمات الرقمية على المؤسسات:

- **سمعة المؤسسة:** يمكن أن تتعرض سمعة المؤسسة لضرر كبير إذا لم تتعامل بسرعة وفعالية مع الأزمة الرقمية، مثل عدم القدرة على حماية بيانات العملاء.
- **الاستمرارية التشغيلية:** قد تتعطل العمليات الأساسية مما يؤدي إلى توقف الأعمال وخسارة الإيرادات.
- **التبعات القانونية والتنظيمية:** قد تواجه المؤسسة غرامات وعقوبات قانونية نتيجة فشلها في حماية البيانات أو التزامها بمعايير الأمن السيبراني.

أولاً: الأزمات الرقمية

4. تأثير الأزمات الرقمية على المؤسسات:

• تدهور السمعة → فقدان الثقة العامة

• توقف العمليات → خسائر فورية

• مساءلة قانونية → غرامات وتنظيمات صارمة

مثال واقعي (2024):

شركة Zain Bahrain تعرضت لانتقادات واسعة بعد تسريب بيانات لعملاء مما أثر على ثقة المستخدمين.

أولاً: الأزمات الرقمية

5. أهمية الاستعداد للأزمات الرقمية:

- **تطوير خطط طوارئ رقمية:** تشمل الخطط التي تتناول كيفية التعامل مع الاختراقات الأمنية، وحماية البيانات، وضمان استمرارية الأعمال.
- **التدريب والتوعية:** تدريب الموظفين على كيفية التعامل مع الأزمات الرقمية وفهم الإجراءات التي يجب اتخاذها عند حدوثها.
- **التعاون مع الجهات المختصة:** التنسيق مع خبراء الأمن السيبراني والجهات التنظيمية لضمان استجابة سريعة وفعالة.

[illegible]

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

أ. تطبيقات الذكاء الاصطناعي في إدارة الأزمات:

1. التنبؤ والتحليل:

• تحليل البيانات الضخمة:

استخدام تقنيات الذكاء الاصطناعي لتحليل كميات هائلة من البيانات من مصادر مختلفة مثل وسائل التواصل الاجتماعي، الأخبار، وتقارير السوق لاكتشاف الأنماط التي قد تشير إلى أزمة محتملة.

التعلم الآلي يمكن أن يتعرف على الاتجاهات والأنماط السابقة التي كانت مرتبطة بأزمات، مما يسمح للمؤسسات بالتحضير لها بشكل أفضل.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

أ. تطبيقات الذكاء الاصطناعي في إدارة الأزمات:

1. التنبؤ والتحليل:

• التنبؤ بالأزمات:

الذكاء الاصطناعي يمكن أن يساعد في التنبؤ بالأزمات قبل حدوثها من خلال نماذج التنبؤ التي تعتمد على البيانات الحالية والتاريخية.

يمكن للتطبيقات مثل الشبكات العصبية التنبؤية التعرف على إشارات مبكرة للهجمات الإلكترونية أو التغيرات في سلوك السوق.

مثال واقعي (2025):

منصة SentiOne AI في السعودية تمكنت من اكتشاف حملات تضليل رقمية ضد جهة حكومية قبل انتشارها.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

أ. تطبيقات الذكاء الاصطناعي في إدارة الأزمات:

2. الاستجابة التلقائية:

تتخذ أنظمة AI إجراءات تلقائية لحماية البيانات أو الرد على العملاء دون تدخل بشري.

مثل استخدام روبوتات الدردشة المدعومة بالذكاء الاصطناعي **Chatbots** للإجابة على استفسارات الجمهور أثناء الأزمات، مما يخفف الضغط عن فرق العلاقات العامة ويضمن استجابة فورية.

هذه الأداة يمكنها معالجة آلاف الطلبات في وقت واحد، مما يجعلها فعالة خلال فترات الذروة.

مثال (2024): شركة **Etihad Airways** استخدمت Chatbots خلال توقف نظام الحجز لتقديم تعليمات فورية للركاب.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

أ. تطبيقات الذكاء الاصطناعي في إدارة الأزمات:

2. الاستجابة التلقائية:

• إدارة الأزمات التلقائية:

أنظمة الاستجابة التلقائية التي يمكن أن تفعل البروتوكولات الخاصة بإدارة الأزمات عند اكتشاف حدث معين، مثل إغلاق الأنظمة المعرضة للخطر أو إرسال تنبيهات إلى الفرق المعنية.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

ب. أمثلة واقعية على استخدام الذكاء الاصطناعي في إدارة الأزمات:

1. التنبؤ بالهجمات الإلكترونية:

دراسة حالة: استخدام الذكاء الاصطناعي في البنوك للكشف المبكر عن الهجمات الإلكترونية.

يتم تطبيق أنظمة الذكاء الاصطناعي لتحليل البيانات المتعلقة بمحاولات الدخول غير المصرح بها والتغيرات غير العادية في حركة الشبكة للتنبؤ بالهجمات الإلكترونية قبل وقوعها.

الفوائد: تمكين المؤسسات من اتخاذ خطوات استباقية لحماية أنظمتها وتقليل الأضرار المحتملة.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

ب. أمثلة واقعية على استخدام الذكاء الاصطناعي في إدارة الأزمات:

2. إدارة الأزمات الصحية:

دراسة حالة: استخدام الذكاء الاصطناعي أثناء جائحة COVID-19.

أنظمة الذكاء الاصطناعي مثل IBM Watson اتم استخدامها لتحليل البيانات الصحية وتقديم تنبؤات حول انتشار الفيروس، بالإضافة إلى تقديم توصيات للحكومات والمؤسسات الصحية.

الفوائد: تحسين الاستجابة للجائحة، توزيع الموارد بكفاءة، وتقليل انتشار الفيروس من خلال تحليل بيانات الاتصال والحركة.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

ب. أمثلة واقعية على استخدام الذكاء الاصطناعي في إدارة الأزمات:

3. التعامل مع الأزمات اللوجستية:

دراسة حالة: تطبيق الذكاء الاصطناعي في سلاسل التوريد خلال الكوارث الطبيعية.

قامت بعض الشركات بتطوير أنظمة تعتمد على الذكاء الاصطناعي لتحليل البيانات الواردة من مئات الموردين والمراكز اللوجستية لتحديد المواقع المحتملة للاختناق وتقديم بدائل في الوقت الحقيقي.

الفوائد: تحسين مرونة سلاسل التوريد وتقليل تأثير الأزمات على العمليات التجارية.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

ج. فوائد وتحديات استخدام الذكاء الاصطناعي في إدارة الأزمات:

1. الفوائد:

السرعة والدقة: الذكاء الاصطناعي يمكن أن يعالج كميات هائلة من البيانات بسرعة ويقدم رؤى دقيقة، مما يساعد المؤسسات على اتخاذ قرارات أسرع وأكثر دقة.

التعامل مع الأزمات بشكل استباقي: من خلال التنبؤ بالأزمات وتحليل الأنماط، يمكن للذكاء الاصطناعي أن يساعد المؤسسات في اتخاذ إجراءات وقائية قبل تفاقم الأزمة.

ثانيًا: دور الذكاء الاصطناعي في إدارة الأزمات

ج. فوائد وتحديات استخدام الذكاء الاصطناعي في إدارة الأزمات:

2. التحديات:

الاعتماد على البيانات: دقة التنبؤات والتحليلات تعتمد على جودة وكميات البيانات المتاحة.

التكلفة والبنية التحتية: تطبيق أنظمة الذكاء الاصطناعي قد يتطلب استثمارات كبيرة في التكنولوجيا والبنية التحتية.

الأخلاقيات والخصوصية: استخدام الذكاء الاصطناعي في تحليل البيانات الحساسة قد يثير قضايا أخلاقية تتعلق بالخصوصية واستخدام المعلومات الشخصية.

The word cloud contains the following terms:

- Crisis**
- Management**
- organization**
- communication**
- process**
- recovery**
- change**
- risk**
- within**
- open**
- successful**
- failure**
- responses**
- throughout**
- perception**
- situations**
- represents**
- crises**
- Power**
- finding**
- ways**
- called**
- probably**
- respectively**
- continuity**
- start**
- constitute**
- serious**
- discipline**
- threat**
- phases**
- accurately**
- Three**
- totally**
- procedures**
- influenced**
- short**
- involve**
- incident**
- occuring**
- putting**
- avoid**
- never**
- time**
- need**
- e.g.**
- skills**
- promot**
- potential**
- terms**
- definition**
- especially**
- quality**
- general**
- defining**
- mitigate**
- respond**
- serious**
- decision**
- common**
- since**
- also**
- site**
- unpredictable**
- occurs**
- point**
- consistent**
- operations**
- related**
- cope**
- deals**
- reputation**
- Therefore**
- Identify**
- reality**
- referred**
- old**
- Venette**
- metrics**
- occurred**
- aid**
- mechanisms**
- challenge**
- consisting**
- transformation**
- Methods**
- Plan**
- context**
- restoration**
- elements**
- contribute**
- focus**
- makes**
- major**
- dealing**
- emergency**
- described**
- element**
- faceted**
- credibility**
- Peter**
- moving**
- necessary**
- term**
- assess**
- business**
- event**
- possible**
- situation**
- businesses**
- used**
- must**
- chances**
- fashion**
- phase**
- untrue**
- catastrophes**
- public**
- trigger**
- techniques**
- surprise**
- required**
- contrast**
- first**
- consequently**
- longer**
- tubing**
- assessing**
- needed**
- specialists**
- fire**
- fourth**
- lived**
- occasionally**
- timely**
- harm**
- moment**
- perception**
- scenarios**
- argue**
- several**
- involved**
- define**
- threatens**
- discipline**
- accurate**
- prompt**
- potential**
- type**
- incidents**
- occurring**
- putting**
- avoid**
- never**
- time**
- need**
- e.g.**
- skills**
- procedures**
- influenced**
- totally**
- Three**
- phases**
- accurately**
- decision**
- common**
- since**
- also**
- site**
- unpredictable**
- occurs**
- point**
- consistent**
- operations**
- related**
- cope**
- deals**
- reputation**
- Therefore**
- Identify**
- reality**
- referred**
- old**
- Venette**
- metrics**
- occurred**
- aid**
- mechanisms**
- challenge**
- consisting**
- transformation**
- Methods**
- Plan**
- context**
- restoration**
- elements**
- contribute**
- focus**
- makes**
- major**
- dealing**
- emergency**
- described**
- element**
- faceted**
- credibility**
- Peter**
- moving**
- necessary**
- term**
- assess**
- business**
- event**
- possible**
- situation**
- businesses**
- used**
- must**
- chances**
- fashion**
- phase**
- untrue**
- catastrophes**
- public**
- trigger**
- techniques**
- surprise**
- required**
- contrast**
- first**
- consequently**
- longer**
- tubing**
- assessing**
- needed**
- specialists**
- fire**
- fourth**
- lived**
- occasionally**
- timely**
- harm**
- moment**
- perception**
- scenarios**
- argue**
- several**
- involved**
- define**
- threatens**
- discipline**
- accurate**
- prompt**
- potential**
- type**
- incidents**
- occurring**
- putting**
- avoid**
- never**
- time**
- need**
- e.g.**
- skills**
- procedures**
- influenced**
- totally**
- Three**
- phases**
- accurately**
- decision**
- common**
- since**
- also**
- site**
- unpredictable**
- occurs**
- point**
- consistent**
- operations**
- related**
- cope**
- deals**
- reputation**
- Therefore**
- Identify**
- reality**
- referred**
- old**
- Venette**
- metrics**
- occurred**
- aid**
- mechanisms**
- challenge**
- consisting**
- transformation**
- Methods**
- Plan**
- context**
- restoration**
- elements**
- contribute**
- focus**
- makes**
- major**
- dealing**
- emergency**
- described**
- element**
- faceted**
- credibility**
- Peter**
- moving**
- necessary**
- term**
- assess**
- business**
- event**
- possible**
- situation**
- businesses**
- used**
- must**
- chances**
- fashion**
- phase**
- untrue**
- catastrophes**
- public**
- trigger**
- techniques**
- surprise**
- required**
- contrast**
- first**
- consequently**
- longer**
- tubing**
- assessing**
- needed**
- specialists**
- fire**
- fourth**
- lived**
- occasionally**
- timely**
- harm**
- moment**
- perception**
- <

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

أ. التحديات التقنية

1. دقة الذكاء الاصطناعي في التعلم والتحليل والتنبؤ:

• نقص البيانات (Data Scarcity)

أنظمة الذكاء الاصطناعي تعتمد على البيانات السابقة وتحتاج إلى كميات ضخمة من البيانات الدقيقة والمتنوعة؛ لتعلم الأنماط والتنبؤ بالأزمات. في الأزمات الجديدة أو غير المتكررة، قد لا تتوفر بيانات كافية لتدريب الأنظمة، مما يجعل نتائجها غير دقيقة أو مضللة؛ ومن ثم تكون بعض الأزمات غير متوقعة تمامًا. إذا كانت البيانات المستخدمة في تدريب النظام محدودة أو غير شاملة، فإن دقة التنبؤات والتحليلات قد تتأثر بشكل كبير.

مثال واقعي (2024):

عند اندلاع أزمة انقطاع الإنترنت في السودان، فشلت بعض أنظمة التحليل المعتمدة على الذكاء الاصطناعي في توقع الاستجابة المجتمعية بسبب غياب البيانات الرقمية المحدثة الناتجة عن طول فترة الحظر.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

أ. التحديات التقنية

1. دقة الذكاء الاصطناعي في التعلم والتحليل والتنبؤ:

• التحيز في الخوارزميات (Algorithmic Bias):

يمكن أن تتأثر نتائج الذكاء الاصطناعي بتحيزات موجودة في البيانات المستخدمة، إذا كانت البيانات المستخدمة في تدريب الذكاء الاصطناعي منحازة ثقافياً أو جغرافياً أو ديموغرافياً، ستعكس الخوارزمية هذا الانحياز في التنبؤات والاستنتاجات فتصبح غير دقيقة أو غير موضوعية؛ مما يؤدي إلى قرارات غير عادلة أو خاطئة خاصة في أثناء الأزمات.

مثال واقعي (2025):

برنامج ذكاء اصطناعي استخدمته إحدى الوزارات العربية لرصد الرأي العام اعتبر انتقادات معينة "سلوكاً عدائياً" بسبب تدريبه على بيانات أجنبية لا تراعي السياق المحلي، مما أدى إلى سوء تفسير المشاعر الرقمية تجاه قرار حكومي.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

أ. التحديات التقنية

1. دقة الذكاء الاصطناعي في التعلم والتحليل والتنبؤ:

• صعوبة تفسير قرارات الذكاء الاصطناعي (Explainability Challenge)

بعض أنظمة الذكاء الاصطناعي، خاصة العميقة منها (مثل الشبكات العصبية)، تعمل بوصفها "صندوقاً أسود" يصعب فهم كيفية وصولها إلى قرار معين، مما يقلل الثقة في نتائجها خلال الأزمات.

مثال واقعي (2024)

إحدى المؤسسات المصرفية الخليجية توقفت عن استخدام نموذج ذكاء اصطناعي للتنبؤ بالاحتيال المالي، لأن النظام أصدر تحذيرات خاطئة دون تفسير منطقي، مما وضع الإدارة في موقف حرج أمام الجهات الرقابية.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

أ. التحديات التقنية

2. الاعتماد على البيانات:

. الكمية والجودة:

أنظمة الذكاء الاصطناعي تعتمد على توفر كميات كبيرة من البيانات الدقيقة والعالية الجودة. إذا كانت البيانات غير متاحة أو غير موثوقة، فقد يؤدي ذلك إلى تحليل غير دقيق. قد تواجه المؤسسات صعوبة في جمع البيانات الكافية في الوقت المناسب، مما يعيق قدرة الذكاء الاصطناعي على التنبؤ بالأزمات.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

أ. التحديات التقنية

2. الاعتماد على البيانات:

• التكامل بين البيانات:

التحدي الآخر يتمثل في كيفية تكامل البيانات من مصادر متعددة (مثل بيانات وسائل التواصل الاجتماعي، بيانات السوق، بيانات التشغيل الداخلي) بشكل فعال لتحقيق تحليل شامل ودقيق.

• التحديث المستمر للبيانات:

من الضروري تحديث البيانات باستمرار لضمان دقة تحليلات الذكاء الاصطناعي. البيانات القديمة أو غير المحدثة يمكن أن تؤدي إلى توقعات غير دقيقة.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

ب. الأخلاقيات والخصوصية

1. مخاوف بشأن استخدام الذكاء الاصطناعي في جمع البيانات وتحليلها:

. المراقبة والتدخل:

يمكن أن يُنظر إلى استخدام الذكاء الاصطناعي في جمع البيانات على أنه تدخل في خصوصية الأفراد، خاصة إذا كانت هذه البيانات تشمل معلومات شخصية حساسة. القلق من أن يتم استخدام أدوات الذكاء الاصطناعي للمراقبة بدلاً من الاستجابة للأزمات، مما يثير قضايا أخلاقية حول حرية الأفراد وحقوقهم.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

ب. الأخلاقيات والخصوصية

1. مخاوف بشأن استخدام الذكاء الاصطناعي في جمع البيانات وتحليلها:

. الشفافية في معالجة البيانات:

هناك حاجة لضمان أن معالجة البيانات من خلال أنظمة الذكاء الاصطناعي تتم بشفافية، وأن الأفراد المعنيين على علم بكيفية استخدام بياناتهم. قد يتطلب ذلك من المؤسسات اعتماد سياسات واضحة ومعلنة حول كيفية استخدام الذكاء الاصطناعي في إدارة الأزمات وحماية البيانات.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

ب. الأخلاقيات والخصوصية

2. حماية المعلومات الشخصية:

. التحديات القانونية والتنظيمية:

هناك تحديات قانونية مرتبطة باستخدام الذكاء الاصطناعي، خاصة فيما يتعلق بحماية المعلومات الشخصية وفقاً للقوانين واللوائح المحلية والدولية مثل GDPR وNCA. المؤسسات تحتاج إلى ضمان امتثالها لهذه القوانين عند استخدام الذكاء الاصطناعي في جمع وتحليل البيانات خلال الأزمات.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

ب. الأخلاقيات والخصوصية

2. حماية المعلومات الشخصية:

. الاختراقات الأمنية:

الاعتماد على الأنظمة الرقمية قد يزيد من مخاطر الاختراقات الأمنية، حيث يمكن للمهاجمين استغلال الثغرات للوصول إلى البيانات الشخصية المخزنة. على المؤسسات اتخاذ تدابير أمنية قوية لضمان حماية البيانات الحساسة من الاختراقات والهجمات السيبرانية.

ثالثاً: التحديات التي تواجه استخدام الذكاء الاصطناعي في إدارة الأزمات

ب. الأخلاقيات والخصوصية

2. حماية المعلومات الشخصية:

• إدارة البيانات المسروقة:

في حالة حدوث خرق للبيانات، يتعين على المؤسسات أن تكون جاهزة للتعامل مع تداعيات مثل هذه الحوادث، والتي قد تشمل استعادة الثقة العامة ومعالجة الأضرار الناتجة عن تسريب المعلومات.

04

رابعاً: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات



رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

أ. تطوير استراتيجيات مرنة

1. دمج الذكاء الاصطناعي في الخطط الشاملة لإدارة الأزمات:

. التخطيط الاستباقي:

يمكن استخدام الذكاء الاصطناعي لتطوير سيناريوهات أزمات محتملة وتخطيط استجابات استباقية. من خلال تحليل البيانات الحالية والتنبؤات، يمكن للمؤسسات إعداد خطط متعددة تتناسب مع مختلف أنواع الأزمات.

يمكن لأنظمة الذكاء الاصطناعي أن تتيح التحليل السريع للبيانات الواردة أثناء الأزمة، مما يسمح باتخاذ قرارات سريعة ومستنيرة.

مثال: هيئة الطيران المدني الإماراتية استخدمت نماذج ذكاء اصطناعي للتنبؤ بازدياد خطوط الطيران وتغيير خطط الطوارئ.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

أ. تطوير استراتيجيات مرنة

2. تعزيز المرونة والقدرة على التكيف:

• تطوير استراتيجيات مرنة:

المرونة هي جوهر أي استراتيجية فعالة لإدارة الأزمات. يجب أن تكون الخطط قادرة على التكيف مع المعلومات الجديدة والظروف المتغيرة، مما يتيح للمؤسسة تغيير مسارها بسرعة إذا لزم الأمر.

الاستفادة من الذكاء الاصطناعي لتحليل البيانات بشكل فوري يساعد في تعزيز المرونة من خلال تقديم توصيات مبنية على الأدلة حول أفضل مسار للعمل.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

أ. تطوير استراتيجيات مرنة

2. تعزيز المرونة والقدرة على التكيف:

- **المرونة في تخصيص الموارد:**
- يمكن لأنظمة الذكاء الاصطناعي مساعدة المؤسسات على تخصيص الموارد بفعالية خلال الأزمات. من خلال تحليل البيانات حول التأثيرات المتغيرة للأزمة، يمكن للمؤسسات توجيه الموارد إلى المناطق الأكثر حاجة.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

أ. تطوير استراتيجيات مرنة

3. تكامل الذكاء الاصطناعي مع الاستراتيجيات القائمة:

. التوافق مع الأنظمة التقليدية:

على الرغم من أن الذكاء الاصطناعي يمكن أن يقدم قيمة كبيرة، فإنه يجب أن يكون متكاملًا مع الأنظمة التقليدية لضمان أن الخطط متجانسة وقابلة للتنفيذ.

يمكن استخدام الذكاء الاصطناعي لتدعيم العمليات التقليدية بدلاً من استبدالها بالكامل، مما يعزز قدرة المؤسسات على إدارة الأزمات بكفاءة. AI لا يحل محل الإنسان، بل يعزز قراراته.

مثال: "البنك الأهلي السعودي" يجمع بين لجان بشرية وأنظمة تنبؤ آلية لرصد الاحتيال المالي.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

أ. تطوير استراتيجيات مرنة

4. إدارة المخاطر المتعلقة بالذكاء الاصطناعي:

• تقليل الاعتماد المفرط:

في حين أن الذكاء الاصطناعي يمكن أن يكون أداة قوية، إلا أن الاعتماد المفرط عليه قد يكون محفوفًا بالمخاطر. من المهم أن تكون هناك خطط بديلة قائمة على العوامل البشرية في حال فشل أنظمة الذكاء الاصطناعي أو تقديمها لتحليلات غير دقيقة.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

أ. تطوير استراتيجيات مرنة

3. إدارة المخاطر المتعلقة بالذكاء الاصطناعي:

• مراجعة الاستراتيجيات بشكل دوري:

يجب مراجعة وتحديث استراتيجيات إدارة الأزمات بشكل دوري لضمان تكامل الذكاء الاصطناعي بأفضل طريقة ممكنة، مع مراعاة التحسينات التكنولوجية والبيانات الجديدة.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي

. أهمية تدريب الفرق:

1. الجاهزية التكنولوجية:

الفرق غير المدربة على AI قد تسبب أزمة أكبر من الأزمة الأصلية. يجب على المؤسسات أن تستثمر في تدريب فرق العمل على استخدام أدوات الذكاء الاصطناعي بفعالية. التدريب المناسب يزيد من جاهزية الفرق ويضمن استفادتهم الكاملة من الإمكانيات التي توفرها التكنولوجيا.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي

. أهمية تدريب الفرق:

2. التفاعل مع التقنية:

الفهم الجيد لكيفية عمل أنظمة الذكاء الاصطناعي يساعد الفرق على التفاعل مع التقنية بشكل أفضل. يتضمن ذلك فهم كيفية تفسير البيانات التي تقدمها أنظمة الذكاء الاصطناعي وكيفية اتخاذ القرارات المستنيرة بناءً عليها.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي

. أهمية تدريب الفرق:

3. التكامل بين الإنسان والآلة:

التدريب يجب أن يركز على التكامل بين العنصر البشري والذكاء الاصطناعي. يمكن للمؤسسات تحقيق أفضل النتائج عندما يتم تعزيز الذكاء الاصطناعي بالخبرة البشرية.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي • برامج التدريب المتخصصة:

1. ورش العمل والندوات:

تنظيم ورش عمل وندوات تدريبية للموظفين حول كيفية استخدام أنظمة الذكاء الاصطناعي في إدارة الأزمات. هذه الورش توفر فرصة للتفاعل المباشر مع التكنولوجيا وتطبيقها في سيناريوهات واقعية.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي • برامج التدريب المتخصصة:

2. التدريب المستمر:

نظرًا للتطور المستمر في تقنيات الذكاء الاصطناعي، يجب أن يكون التدريب مستمرًا. يمكن تحقيق ذلك من خلال برامج تطوير مهني مستمرة تهدف إلى إبقاء الفرق على اطلاع بأحدث المستجدات.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي • برامج التدريب المتخصصة:

3. التدريب العملي:

تقديم تدريبات عملية تساعد الفرق على تجربة الأدوات التكنولوجية في بيئات محاكاة للأزمات، مما يزيد من مستوى الثقة والكفاءة في استخدامها عند الحاجة الفعلية.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي . بناء فرق متعددة التخصصات:

1. التعاون بين الأقسام:

لتفعيل استراتيجيات الذكاء الاصطناعي بنجاح، من الضروري وجود فرق عمل متعددة التخصصات تشمل خبراء في التكنولوجيا، إدارة الأزمات، والاتصال. هذا التكامل يساهم في تطبيق استراتيجيات أكثر فعالية.

رابعًا: استراتيجيات دمج الذكاء الاصطناعي في خطط إدارة الأزمات

ب. تدريب الفرق على استخدام الذكاء الاصطناعي
. بناء فرق متعددة التخصصات:

2. التنسيق المستمر:

التنسيق المستمر بين الأقسام المختلفة يضمن أن جميع الجوانب المتعلقة بالأزمة تُدار بشكل متكامل وفعال، مع الاستفادة الكاملة من إمكانيات الذكاء الاصطناعي.

05

خامسًا: دراسة حالة: إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي



خامساً: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

1. AI Misuse Crisis Management (OpenAI)

كيف تدير المؤسسة إساءة استخدام الذكاء الاصطناعي؟

الحالة 1: OpenAI واكتشاف حملات التأثير المدعومة بالذكاء الاصطناعي (2025)

في يونيو 2025 نشرت OpenAI تقريرها الدوري عن إساءة استخدام الذكاء الاصطناعي، وكشفت عن عدة حملات تأثير رقمية (Influence Operations) استخدمت نماذجها لإنتاج محتوى مضلل، وإدارة حسابات وهمية، وإنشاء منشورات ومقالات بلغات متعددة بهدف التأثير على الرأي العام، ودعم عمليات تضليل إلكتروني وحملات هندسة اجتماعية.

لم تكن الأزمة اختراقاً تقنياً للنظام، وإنما تمثلت في إساءة استخدام منتجات الشركة بطريقة تهدد الثقة العامة في تقنيات الذكاء الاصطناعي.

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

الحالة 1: OpenAI واكتشاف حملات التأثير المدعومة بالذكاء الاصطناعي (2025)

استخدام الذكاء الاصطناعي:

- استخدمت OpenAI أنظمة مراقبة داخلية لاكتشاف أنماط الاستخدام غير الطبيعية لنماذجها.
- قامت بتحليل المحادثات والمخرجات المرتبطة بالحسابات المشبوهة لتحديد طبيعة النشاط.
- أغلقت الحسابات المستخدمة في حملات التأثير الخبيثة قبل توسعها.
- نشرت تقريرًا تفصيليًا يوضح أساليب المهاجمين وآليات الكشف والاستجابة، في إطار تعزيز الشفافية وبناء الثقة مع المستخدمين وصناع القرار.

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

الحالة 1: OpenAI واكتشاف حملات التأثير المدعومة بالذكاء الاصطناعي (2025) النتيجة

- سرعة الاكتشاف: احتواء عدد من حملات التضليل قبل تحقيق انتشار واسع.
- الحد من الأضرار: تحسين قدرة المؤسسة على رصد الاستخدامات الضارة للذكاء الاصطناعي.
- استعادة الثقة: تعزيز الثقة من خلال الإفصاح العلني عن الحوادث والإجراءات التصحيحية.

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

الحالة 1: OpenAI واكتشاف حملات التأثير المدعومة بالذكاء الاصطناعي (2025)

الدروس المستفادة:

- لا تقتصر إدارة الأزمات على الاستجابة بعد وقوع الأزمة، بل تشمل الاكتشاف المبكر والوقاية.
- تمثل الشفافية والإفصاح المنظم عنصرين أساسيين في إدارة السمعة الرقمية.
- ينبغي أن تتضمن خطط إدارة الأزمات آليات لرصد إساءة استخدام تقنيات الذكاء الاصطناعي، حتى عندما تكون المؤسسة نفسها مطورة لهذه التقنيات.

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

دراسة حالة 2:

هيئة كهرباء ومياه دبي DEWA وإدارة أزمة تضليل رقمي باستخدام الذكاء الاصطناعي (2025)

أ. تحليل دراسة الحالة

نوع الأزمة: حملة تضليل رقمي Disinformation Campaign تستهدف التشكيك في دقة الفواتير الإلكترونية وزيادات غير حقيقية في الرسوم.

وصف الأزمة: في يناير 2025، انتشرت عبر منصات التواصل الاجتماعي شائعات تدعي أن هيئة كهرباء ومياه دبي رفعت رسوم الاستهلاك بنسبة 40٪ دون إعلان رسمي. وتضمنت الحملة صورًا مزيفة لفواتير معدلة، مما تسبب في:

- موجة غضب بين العملاء
- ارتفاع ملحوظ في الاتصالات مع مراكز الخدمة
- تداول مكثف للخبر في أقل من 3 ساعات

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

هيئة كهرباء ومياه دبي DEWA وإدارة أزمة تضليل رقمي باستخدام الذكاء الاصطناعي (2025)
أ. تحليل دراسة الحالة

استخدام الذكاء الاصطناعي في إدارة الأزمة:

- إطلاق فيديو توضيحي يشرح آلية احتساب الفاتورة
- نشر بيانات رسمية عبر القنوات الرقمية وخدمة الرد الآلي
- استخدام لوحة Dashboard AI لقياس التفاعل وتصحيح المفاهيم
- تقديم محاكٍ تفاعلي يتيح للمستخدم حساب فاتورته بنفسه

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

هيئة كهرباء ومياه دبي DEWA وإدارة أزمة تضليل رقمي باستخدام الذكاء الاصطناعي (2025)

أ. تحليل دراسة الحالة

نتائج استخدام الذكاء الاصطناعي في إدارة الأزمة:

- انخفاض الشائعات بنسبة 62% في أقل من 24 ساعة
- انخفاض الاستفسارات والبلاغات بنسبة 38% خلال يومين
- تعزيز ثقة الجمهور عبر شفافية البيانات
- اعتبرت هذه الاستجابة نموذجًا خليجيًا في إدارة حملات التضليل الرقمية المعتمدة على AI

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

هيئة كهرباء ومياه دبي DEWA وإدارة أزمة تضليل رقمي باستخدام الذكاء الاصطناعي (2025)

أ. تحليل دراسة الحالة

المرحلة	دور الذكاء الاصطناعي	دور الذكاء الاصطناعي في إدارة الأزمة
رصد المحتوى	تحليل ملايين المنشورات على X سابقاً و TikTok و Reddit	اكتشاف مصدر الشائعة الأساسي
تحليل البيانات	تحديد الحسابات المحركة للحملة وارتباطها بمصادر خارجية	كشف الدافع وراء التضليل
الاستجابة الاستراتيجية	إنتاج رسائل مرئية وبيانات رسمية مدعومة بالأرقام	إيقاف انتشار المعلومات المضللة

خامسًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

هيئة كهرباء ومياه دبي DEWA وإدارة أزمة تضليل رقمي باستخدام الذكاء الاصطناعي (2025)
ب. دروس مستفادة

أهمية الاستعداد المسبق: يظهر المثال أهمية وجود أنظمة ذكاء اصطناعي متطورة للتحليل والاستجابة. الذكاء الاصطناعي لا يكتشف الشائعات فحسب، بل يفككها ويواجهها بالبيانات. في عصر المعلومات، الحقيقة لا تنتصر بالصمت... بل بالأرقام.

حَامِشًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

3. Deepfake Crisis Management

كيف تدير المؤسسة أزمة ناتجة عن انتحال الهوية بالذكاء الاصطناعي؟

الحالة 3: هجوم Deepfake على شركة WPP باستخدام انتحال هوية رئيسها التنفيذي (2025)

في مايو 2025 أعلن الرئيس التنفيذي لشركة WPP، Mark Read، عن تعرض الشركة لمحاولة احتيال متقدمة استخدمت الذكاء الاصطناعي التوليدي. أنشأ المهاجمون نسخة مزيفة (Deepfake) من صوته وصورته خلال اجتماع عبر Microsoft Teams مع حسابات بريد إلكتروني ووثائق مزيفة، في محاولة لإقناع أحد المديرين التنفيذيين بتحويل أموال والكشف عن معلومات حساسة.

حَامِشًا: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

الحالة 3: هجوم Deepfake على شركة WPP باستخدام انتحال هوية رئيسها التنفيذي (2025)

استخدام الذكاء الاصطناعي:

- أوقفت الشركة العملية فور اكتشاف مؤشرات الانتحال.
- أصدرت تحذيرًا داخليًا لجميع الموظفين يشرح تفاصيل الهجوم وأساليبه.
- عززت إجراءات التحقق من الهوية في الاجتماعات الافتراضية والتحويلات المالية.
- كثفت برامج التدريب والتوعية حول مخاطر Deepfake والهندسة الاجتماعية.
- استخدمت الحادثة لدمج أدوات كشف التزييف ضمن منظومة الأمن السيبراني، وتحديث سياسات الأمن السيبراني وإدارة الأزمات الرقمية.

خاتمة: دراسة حالة إدارة أزمة إلكترونية باستخدام الذكاء الاصطناعي

الحالة 3: هجوم Deepfake على شركة PP باستخدام هوية رئيسها التنفيذي

النتيجة

- احتواء الأزمة: لم تنجح محاولة الاحتيال في تحقيق أهدافها نتيجة سرعة اكتشافها.
- تعزيز الجاهزية: دفعت الحادثة الشركة إلى تحديث سياسات التحقق وإدارة المخاطر الرقمية.
- رفع الوعي: أصبحت الحادثة جزءاً من برامج التدريب الداخلي على الأمن السيبراني وإدارة الأزمات.

الدروس المستفادة:

- لم يعد الصوت أو الفيديو دليلاً كافياً للتحقق من الهوية.
- أصبحت هجمات Deepfake تمثل تهديداً مباشراً لإدارة الأزمات والاتصال المؤسسي.
- يجب أن تتكامل إدارة العلاقات العامة مع الأمن السيبراني وإدارة المخاطر عند التعامل مع هذا النوع من الأزمات.
- تمثل التوعية المستمرة للموظفين وخطط التحقق متعددة المستويات خط الدفاع الأول ضد الهجمات المدعومة بالذكاء الاصطناعي.

إدارة الأزمات في عصر الرقمنة والذكاء الاصطناعي

دور الذكاء الاصطناعي
في إدارة الأزمات

استراتيجيات دمج
الذكاء الاصطناعي
في خطط إدارة
الأزمات



الأزمات الرقمية

التحديات التي تواجه
استخدام الذكاء
الاصطناعي في
إدارة الأزمات

دراسة حالة: إدارة أزمة إلكترونية
باستخدام الذكاء الاصطناعي



Thank You