Abstract

Digitalization and new technologies have become increasingly integral to the operations of humanitarian organizations. As these organizations embrace new digital technologies, they transition from passive participants to active stakeholders in the realm of cyberspace. However, this increased involvement also exposes them to potential cyber threats that can undermine their ability to protect and aid individuals affected by armed conflicts or violence. Therefore, humanitarian organizations must comprehend the security risks associated with these advanced technologies to safeguard their systems and data. Security in this context encompasses the interplay of people, processes, and technology.

Information Security Awareness (ISA) has gained significant attention as a concept that can mitigate the risks posed by information security breaches. Numerous ISA models have been developed to address this need. However, existing models have not adequately addressed the specific needs of humanitarian organizations. This research proposes an Enhanced Information Security Awareness model for humanitarian organizations, which includes two additional focus areas: device securement and awareness of policy. The enhanced model builds upon the existing seven focus areas in addition to the two added focus areas and aims to provide a comprehensive framework tailored to the unique challenges faced by humanitarian organizations.

The effectiveness of the enhanced model was evaluated using the EHAIS-Q questionnaire. The results of the thesis indicate that the inclusion of the two additional focus areas in the enhanced model has positively influenced information security awareness within humanitarian organizations. The findings also demonstrate that the enhanced model effectively enhances employees' understanding of information security, leading to an improved security culture within humanitarian organizations.

In conclusion, the proposed Enhanced Information Security Awareness model, with its additional focus areas of device securement and awareness of policy, fills the gap in addressing the specific needs of humanitarian organizations. The research findings highlight the positive impact of the enhanced model on information security awareness and emphasize its effectiveness in enhancing employees' understanding of information security practices.

الملخص

أصبحت التقنيات الجديدة جزءًا لا يتجزأ من عمليات المنظمات الإنسانية. ومع تبني هذه المنظمات للتقنيات الرقمية الجديدة، فإنها تنتقل من المشاركين السلبيين إلى أصحاب المصلحة النشطين في عالم الفضاء الإلكتروني. ومع ذلك، فإن هذه المشاركة المتزايدة تعرضهم أيضًا لتهديدات إلكترونية محتملة يمكن أن تقلل قدرتهم على حماية ومساعدة الأفراد المتضررين. ولذلك، من الضروري أن تدرك المنظمات الإنسانية المخاطر الأمنية المرتبطة بهذه التقنيات المتقدمة من أجل حماية أنظمتها وبياناتها. يشمل الأمن في هذا السياق التفاعل بين الأشخاص والعمليات والتكنولوجيا.

لقد اكتسب الوعي بأمن المعلومات اهتمامًا كبيرًا كمفهوم يمكن أن يخفف من المخاطر التي تشكلها انتهاكات أمن المعلومات. وقد تم تطوير العديد من نماذج لتلبية هذه الحاجة. ومع ذلك، فإن النماذج الحالية لم تعالج بشكل كاف الاحتياجات المحددة للمنظمات الإنسانية. يقترح هذا البحث نموذجًا محسناً للتوعية بأمن المعلومات للمنظمات الإنسانية، والذي يتضمن مجالين إضافيين للتركيز: تأمين الأجهزة والوعي بالسياسات. يعتمد النموذج المعزز على مجالات التركيز السبعة الحالية بالإضافة إلى مجالي التركيز الإضافيين ويهدف إلى توفير إطار شامل مصمم خصيصًا للتحديات الفريدة التي تواجهها المنظمات الإنسانية.

تم تقييم فعالية النموذج المحسن باستخدام استبيان EHAIS-Q. تشير نتائج الرسالة إلى أن إدراج مجالي التركيز الإضافيين في النموذج المعزز قد أثر بشكل إيجابي على الوعي بأمن المعلومات داخل المنظمات الإنسانية. وتوضح النتائج أيضًا أن النموذج المعزز يعزز بشكل فعال فهم الموظفون لأمن المعلومات، مما يؤدي إلى تحسين الثقافة الأمنية داخل المنظمات الإنسانية.

في الختام، فإن نموذج الوعي المعزز بأمن المعلومات، مع مجالات التركيز الإضافية الخاصة بتأمين الأجهزة والوعي بالسياسة، يسد الفجوة في تلبية الاحتياجات المحددة للمنظمات الإنسانية. وتسلط نتائج البحث الضوء على الأثر الإيجابي للنموذج المعزز في الوعي بأمن المعلومات والتأكيد على فعاليته في تعزيز فهم الموظفين لممارسات أمن المعلومات.