

ABSTRAK

Saat ini penggunaan sistem informasi telah menjadi suatu kebutuhan yang penting bagi sebuah organisasi, termasuk salah satunya di lingkungan penyedia layanan kesehatan, yaitu rumah sakit. Kemampuan untuk mengakses, memanfaatkan dan menyediakan informasi secara tepat dan akurat menjadikan pentingnya keamanan informasi bagi rumah sakit.

Informasi di rumah sakit diperlukan pengamanan untuk menjaga kebenaran dan nilai yang dimiliki supaya tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Informasi kesehatan di rumah sakit mengalami pelanggaran keamanan (*security breach*) yang tinggi karena dianggap lebih berharga daripada data kartu kredit. Penyebab utama pelanggaran keamanan ini adalah akses tidak sah (*unauthorized access*) dari pihak internal di perusahaan.

Rumah sakit harus menciptakan budaya keamanan informasi untuk mengurangi jumlah pelanggaran keamanan dan melindungi informasi kesehatan pasien mereka. Penelitian ini bertujuan untuk menganalisis budaya keamanan informasi di rumah sakit. Keberadaan sistem Jaminan Kesehatan Nasional mewajibkan rumah sakit yang terdaftar di Badan Penyelenggara Jaminan Sosial (BPJS) untuk menggunakan setidaknya satu sistem *online* untuk mengelola data milik pasien.

Penelitian menggunakan sampel sejumlah rumah sakit di Kota Bandung. Metode penelitian adalah metode kuantitatif dengan teknik analisis data *Partially Least Square Structural Equation Modelling* (PLS-SEM). Data penelitian adalah data primer melalui kuisioner untuk sejumlah pegawai rumah sakit. Berdasarkan penelitian terdahulu, budaya keamanan informasi dipengaruhi oleh berbagai faktor dan budaya organisasi secara keseluruhan. Penelitian diharapkan memberikan wawasan tentang budaya keamanan informasi di rumah sakit Kota Bandung dan mendukung strategi e-kesehatan nasional oleh Kementerian Kesehatan Republik Indonesia.

Penelitian ini dimulai dengan jumlah variabel sebanyak 14, yaitu *management, workplace capabilities, risk and response factors, operational management, change management, organisational culture, knowledge, security compliance, security behavior, soft issues – workplace independent, training and awareness, information security policies, perceived security threat* dan *attitude*. Namun, ternyata yang berpengaruh terhadap *Information Security Culture (ISC)* adalah *organisational culture, knowledge, information security policies, perceived security threat* dan *attitude*.

Kata kunci: Keamanan Informasi, budaya, rumah sakit.