



## Abstrak

Organisasi menghadapi ancaman yang bersifat kompleks, ambigu, penuh ketidakpastian dan mudah berubah. Organisasi harus memenuhi tuntutan akan teknologi informasi dan mengelola organisasi. Masalah keamanan informasi muncul karena kerentanan jaringan internet dan perilaku. Dampak dari resiko keamanan informasi adalah kerugian finansial, reputasi buruk dan ancaman kesinambungan organisasi, dan hilangnya kepercayaan pada pembayaran dengan sistem *online*. Pengatasan masalah keamanan informasi hanya mengandalkan teknologi, belum ada yang menggunakan konteks sosio-teknis.

*Normal accident theory* menjadi dasar dalam menganalisis kecelakaan di industri. *Human error model* menjelaskan terjadinya kesalahan akibat manusia dan sistem dalam kecelakaan kerja. Terjadi perubahan fokus masalah *safety* semula pada organisasi industri berisiko tinggi berbasis tenaga manusia menuju permasalahan *safety* pada organisasi berbasis teknologi informasi yang juga berisiko tinggi.

Pendekatan *grounded research dan multiple case study* digunakan untuk mengembangkan teori yang menjelaskan terjadinya “celaka” pada organisasi berbasis teknologi informasi. Tujuan penelitian ini adalah menjelaskan proses mengembangkan iklim keamanan informasi pada organisasi berbasis teknologi informasi. Organisasi kasus meliputi organisasi pemerintahan, perbankan, swasta penyedia jaringan, asuransi, dan perguruan tinggi. Proposisi yang dikembangkan adalah : iklim organisasi berbasis *non information technology* berbeda dengan iklim organisasi yang berbasis teknologi informasi; perubahan hubungan organisasi dengan lingkungan diakibatkan teknologi yang diadopsi; sistem teknis dan sistem sosial mengantar teknologi sampai pada manusia ; wujud keamanan informasi adalah kehati-hatian, akuntabilitas, kepekaan terhadap etik, dan integritas: tipe proses pengembangan iklim keamanan informasi dipengaruhi konteks sosial, organisasi, individu dan teknologi.

**Key word:** iklim organisasional, iklim keamanan informasi, organisasi berbasis teknologi informasi

## Abstract

Organizations are facing threats that are complex, ambiguous, full of uncertainty, and evolving. Organizations must fulfill the demand for information technology and organizational management. The issue of information security emerges because of internet connection vulnerability and behaviors. The impact of information security risks are financial loss, tarnished reputation, and the threat of organization collapse, and the loss of trust on online payment. So far organizations issues have only relied on technology to resolve information security issues, no one has ever used a socio-technical context.

*Normal accident theory* has become the basis in analyzing accidents in industries. *Human error model* explains the occurrence of human error mistakes and the system in work place accidents. There has been a shift of focus regarding safety issues in human based high risk industry organization to safety issues in information technology based high risk organizations.

The grounded research and multiple case study approach is used to develop a theory that could explained the “accidents” in information technology based organization. The aim of this research is to develop information security climate in information technology based organizations. The case organizations comprises of organizations like government, banks, private network services, insurance, and universities. The developed proposition is: non information technology based organizational climate is different than information technology based organizational climate; the changes in the relationship between organizations with the environment is caused by the adopted technology; technical and social systems take technologies to human; the form of information securities are caution, accountability, ethic awareness, and integrity; the type of information security climate development process depend on the social, organizational, individual, and technological context.

**Key words:** organizational climate, information security climate, information technology based organization