BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Penggunaan teknologi komunikasi dan informasi yang semakin tinggi telah membawa dampak positif bagi kehidupan berorganisasi. Namun, ketergantungan pada teknologi tersebut juga membuat organisasi menghadapi berbagai risiko. Salah satu risikonya adalah peretasan dan pencurian data (Green & Dorey, 2016). Teknologi komunikasi dan informasi memiliki peran vital bagi keberlangsungan bisnis, baik yang kecil, menengah, sampai ke perusahaan multinasional. Beberapa fungsi teknologi komunikasi dan informasi dalam organisasi antara lain sebagai media komunikasi antara staf, *supplier* dan klien, sistem manajemen inventaris, sistem manajemen data, dan manajemen relasi klien (MacKechnie, 2019). Fungsi teknologi informasi tersebut telah membantu organisasi untuk menghemat tenaga, waktu, dan biaya sehingga alur kerjanya bisa berjalan secara lebih efisien dan efektif. Sayangnya dengan peran teknologi yang besar, risiko peretasan dan pencurian data bisa menyerang organisasi tanpa waktu yang dapat diprediksi juga semakin besar.

Pada kasus peretasan dan pencurian data, Green & Dorey (2016) mengatakan bahwa *human is the weakest link*. Manusia diumpamakan sebagai mata rantai terlemah ketika serangan oleh *hackers* terjadi. Ibaratnya anggota internal organisasi adalah mata rantai yang saling berkaitan. Jika ada satu saja mata rantai yang terbuka, maka kesatuan rantai akan terputus. Hal ini disebabkan oleh modus kejahatannya yang memanfaatkan keterlibatan pihak internal organisasi secara tidak sadar. Modus kejahatan tersebut adalah dengan mengirimkan *email* jebakan yang seolah-olah terlihat seperti *email* profesional.

Dalam dunia IT*, email* jebakan seperti ini disebut dengan istilah *phishing mail* (Green & Dorey, 2016). Melalui *phishing mail,* banyak anggota internal organisasi atau perusahaan yang terkecoh untuk memasukkan data sensitif seperti

password, *username*, alamat, dan sebagainya ke dalam *link* jebakan yang dipasang oleh *hackers.* Walaupun divisi IT sudah membangun sistem keamanan yang kuat, jika ada anggota internal yang memberikan data sensitif melalui *phishing mail,* maka *hackers* akan mendapatkan akses untuk masuk ke dalam sistem informasi dan komunikasi organisasi.

Banyak perusahaan yang menyangkal kondisi *cyber security* yang mereka alami karena masih banyak pelaku bisnis dan organisasi yang kurang pengetahuan mengenai seberapa jauh ancaman *cyber* ini bisa berdampak pada perusahaan. Beberapa pelaku bisnis merasa bahwa ada banyak hal yang lebih penting untuk dipikirkan demi keberlangsungan bisnis sehingga mereka mengesampingkan pentingnya membangun sistem keamanan *cyber* yang kuat. Mereka juga merasa yakin bahwa peretasan yang berdampak besar tidak akan mungkin menimpa bisnis mereka (Green & Dorey, 2016).

Berbeda dengan perusahaan dan organisasi yang belum sadar akan dampak peretasan teknologi informasi dan komunikasi, *International Organization for Migration* (IOM) merupakan salah satu organisasi yang sudah melek terhadap isu ini dan serius dalam melakukan pencegahan peretasan dan pencurian data. IOM adalah sebuah *Intergovernmental Organization* (IGO) yang berada di bawah naungan *United Nations* (UN). IOM bertugas untuk menyediakan jasa pelayanan dan konsultasi perihal imigrasi kepada pemerintah dan para imigran. Dalam menjalankan tugasnya, IOM dihadapi oleh ancaman yang memiliki potensi untuk menghambat kinerja stafnya, mencemarkan nama baik organisasi, dan mengancam keselamatan para klien. Ancaman tersebut adalah upaya *cybercrime* dalam bentuk peretasan dan pencurian data sensitif organisasi yang dilakukan oleh para *hackers*.

Sebagai organisasi internasional yang bergerak dalam bidang kemanusiaan, IOM mendapat dukungan dana yang berasal dari pemerintah maupun swasta. IOM memiliki tanggung jawab untuk mengomunikasikan segala perkembangan kegiatan organisasinya kepada pemerintah, donatur, imigran, staf, dan *stakeholders* lainnya. Maka dari itu IOM memanfaatkan teknologi informasi dan komunikasi seperti *website*, *intranet, e-mail*, dan media sosial untuk menyebarkan informasi mengenai

berbagai perkembangan kegiatan organisasi. IOM juga menyimpan data-data pribadi para imigran dan *stakeholders* dalam sistem komputer organisasi agar lebih mudah untuk diakses dan diolah oleh stafnya. Senada dengan apa yang dikatakan oleh Green dan Dorey, meskipun keberadaan teknologi informasi dan komunikasi mempermudah kehidupan berorganisasi, namun dari sini juga lah tercipta celah bagi peretas untuk menembus akses sistem keamanan IOM (Green & Dorey, 2016).

Peretasan dan pencurian data adalah masalah global yang telah menyebabkan kerugian ekonomi secara besar-besaran di seluruh dunia (Weisbaum, 2018). Selain kerugian finansial, reputasi organisasi pun dapat terancam jika mereka tidak bisa mengendalikan serangan *cyber* yang dilakukan oleh *hackers.* Penelitian telah menunjukkan bahwa sepertiga pelanggan ritel, keuangan, dan perawatan kesehatan akan berhenti berbisnis dengan organisasi yang telah mengalami peretasan dan pencurian data. Selain itu, perusahaan yang pernah mengalami insiden ini sering kali mengalami peningkatan biaya saat harus mendapatkan pelanggan baru. Hal ini disebabkan oleh hilangnya kepercayaan pelanggan terhadap perusahaan tersebut. Pelanggan akan merasa tidak aman lagi untuk memberikan data pribadinya ke perusahaan yang tidak bisa menjaganya dari peretasan dan pencurian oleh *hackers* (Ismail, 2018).

Dalam kasus-kasus yang pernah dialami IOM, peretasan data dilakukan untuk melumpuhkan sistem informasi dan komunikasi organisasi. Seperti yang telah dijelaskan sebelumnya bahwa teknologi informasi dan komunikasi memiliki peran krusial dalam keberlangsungan organisasi, salah satunya sebagai media komunikasi antara staf dan para *stakeholders* lainnya (MacKechnie, 2019). Jika sistem informasi dan komunikasi dilumpuhkan, maka akan menghambat kegiatan operasi organisasi. Apabila kelumpuhan sistem informasi dan komunikasi ini berlangsung terlalu lama, maka akan mengakibatkan kerugian ekonomi dan reputasi. Ketika terjadi kelumpuhan sistem informasi dan komunikasi, IOM tidak dapat melakukan komunikasi dan menyebarkan informasi kepada para *stakeholders*. Begitu pula dengan para *stakeholders*, ketika sistem sedang lumpuh, mereka tidak dapat mengakses media sosial, *e-mail*, dan *website* IOM untuk

mendapatkan informasi yang mereka inginkan. Pihak IOM khawatir jika kejadian ini sering terjadi, maka para *stakeholders* akan meragukan kredibilitas dan transparansi organisasi karena keterbatasan informasi dan komunikasi tersebut.

Selain lumpuhnya sistem informasi dan komunikasi, data pribadi para klien pun bisa terancam keamanannya. IOM cenderung memiliki resiko lebih tinggi dari perusahaan lain jika sistem informasinya berhasil dipenetrasi oleh *hackers*. Selain kerugian ekonomi dan reputasi, keselamatan nyawa klien dapat terancam jika informasi pribadinya tersebar. IOM bertanggungjawab untuk menjaga kerahasiaan data pribadi seluruh imigran yang menjadi kliennya.

Selain harus melindungi data para imigran, IOM juga harus melindungi data pribadi *stakeholders* lainnya seperti, donatur, pemerintah, maupun pihak swasta yang ikut serta mendukung misi kemanusiaan IOM. Jika data pribadi mereka jatuh ke pihak yang salah, maka besar kemungkinannya data mereka akan disalahgunakan. Jika hal itu terjadi, reputasi IOM akan terancam karena dianggap tidak dapat melindungi privasi klien.

Modus penipuan untuk meretas dan mencuri data oleh para *hackers* di IOM dilakukan dengan cara yang sama seperti yang dipaparkan Green & Dorey (2016), yaitu dengan mengirim *phising mail* ke *email* para staf IOM. *Phishing mail* ini sering menyamar seperti *email* bisnis dari perusahaan-perusahaan rekan kerja IOM (seperti Amazon dan SAP). Hal ini membuat beberapa staf percaya bahwa *e-mail* tersebut dikirim dengan tujuan bisnis.

Ketika para staf menerima *email* yang mereka kira adalah *e-mail* bisnis, mereka akan membuka *email* tersebut dan mengakses *link* jebakan yang dicantumkan di dalamnya. Biasanya *link* tersebut akan mengarahkan staf untuk mengisi informasi sensitif seperti *user id, password*, dan nomor kartu kredit. Jika ada staf yang memberikan informasi sensitif tersebut, maka akses bagi *hackers* untuk masuk ke dalam sistem informasi dan komunikasi IOM akan terbuka.

Menurut Green & Dorey (2016), walaupun konfliknya terjadi dalam bidang IT, namun hal terpenting dalam mencegah terjadinya peretasan dan pencurian data

organisasi adalah dengan mengadakan program komunikasi atau sosialisasi kepada para anggota organisasi. Mereka juga mengatakan bahwa sistem keamanan *cyber* secanggih dan semahal apapun akan percuma jika para anggotanya tidak teredukasi dan terbiasa untuk menerapkan penggunaan teknologi informasi dan komunikasi sesuai dengan kebijakan yang berlaku. Ismail (2018) juga mengatakan bahwa perusahaan sebaiknya berinvestasi dalam pendidikan karyawan. Perusahaan harus melatih karyawannya untuk mengidentifikasi *e-mail* dan berkas berbahaya. Hal tersebut akan membantu mencegah organisasi menjadi korban serangan *hackers*. Senada dengan yang dikatakan oleh Green, Dorey, dan Ismail, IOM juga mengadakan program komunikasi internal dalam rangka mengedukasi staf nya untuk mencegah terjadinya peretasan dan pencurian data.

Seiring berjalannya waktu, *corporate communication* memiliki fungsi-fungsi baru. Ketika *stakeholder* mulai menuntut informasi yang lebih dalam dan spesifik dari organisasi, praktisi komunikasi mulai melihat komunikasi organisasi sebagai sesuatu yang lebih besar dari *public relations.* Salah satu fungsi baru tersebut adalah komunikasi internal. *Corporate communication* dapat diartikan sebagai fungsi manajemen yang bertanggung jawab untuk mengawasi dan mengkoordinasi pekerjaan yang dilakukan oleh praktisi komunikasi dalam disiplin ilmu yang berbeda, salah satunya adalah komunikasi internal (Cornelissen, 2017). Pada intinya, strategi komunikasi terdiri dari bagaimana praktisi komunikasi memandu desain dan perencanaan program komunikasi organisasi.

Program komunikasi internal IOM dimotivasi oleh fakta bahwa bahkan sampai sekarang, para staf masih sering mendapatkan *phishing mail* dari *hackers* yang mencoba masuk ke dalam sistem keamanan organisasi, dan masih ada staf yang terjebak dengan pancingan para *hackers.* Hal ini menunjukkan bahwa ancaman peretasan dan pencurian data ini memang berasal dari pihak eksternal, namun yang tanpa sadar memberikan akses kepada para peretas sampai bisa masuk ke sistem informasi dan komunikasi organisasi adalah pihak internal IOM itu sendiri. Maka dari itu IOM memutuskan untuk membuat program komunikasi tersebut.

Dalam kehidupan berorganisasi, komunikasi memiliki peran penting dalam menggerakkan para anggotanya untuk mencapai suatu tujuan tertentu. Salah satu tujuan komunikasi dalam organisasi adalah untuk mengedukasi para anggotanya agar tercipta sebuah kultur tertentu yang diharapkan oleh para petingginya (Robbins & Judge, 2014). Program komunikasi dengan tujuan tersebut diterapkan oleh IOM sebagai bentuk upaya untuk memberikan pemahaman kepada para stafnya tentang adanya ancaman peretasan dan pencurian data, serta protokol-protokol yang harus diikuti untuk mencegahnya.

Pada program komunikasi internal IOM, pemahaman yang berusaha dikomunikasikan diharapkan dapat berujung pada pembentukan kultur, dimana para staf mampu mencegah terjadinya peretasan dan pencurian data organisasi secara mandiri. IOM menciptakan program komunikasi internal untuk mengedukasi dan mengarahkan staf nya agar lebih siaga dan bijak dalam menggunakan teknologi informasi dan komunikasi organisasi, sehingga tidak mudah terkecoh dengan pancingan-pancingan yang dikirimkan oleh *hackers*.

Program komunikasi tersebut telah dilakukan oleh IOM sejak lima tahun yang lalu, dan akan selalu dilakukan di masa depan. Hal ini disebabkan oleh teknologi yang terus berkembang. *Hackers* pun akan selalu memperbarui modus kejahatannya, sehingga protokol keamanan yang sebelumnya sudah disosialisasikan belum tentu dapat mencegah modus kejahatan yang baru. IOM tidak dapat mengontrol apa yang akan dilakukan oleh *hackers*, tetapi IOM bisa membangun sistem pertahanan yang kuat dengan mengedukasi para stafnya. Sejak pertama kali program komunikasi internal diberlakukan, jumlah karyawan yang terjebak dengan *email* peretas semakin berkurang. Hal tersebut telah membantu IOM untuk mencegah ancaman peretasan dan pencurian data ini berkembang menjadi krisis yang lebih besar. Artinya program komunikasi internal yang dilakukan IOM telah berhasil mengedukasi stafnya untuk mencegah peretasan dan pencurian data oleh para *hackers*.

Berdasarkan pemaparan di atas, penulis ingin meneliti strategi perencanaan program komunikasi internal yang dilakukan IOM dalam upaya mengedukasi

stafnya untuk mencegah peretasan dan pencurian data siber organisasi. Keberhasilan program komunikasi internal yang dilakukan IOM menjadi daya tarik bagi penulis untuk meneliti strategi perencanaannya.

Peneliti ingin mengetahui lebih dalam bagaimana IOM merencanakan program komunikasi internal yang telah berhasil meningkatkan pemahaman stafnya mengenai risiko, serta cara mencegah peretasan dan pencurian data. Peneliti dapat menggali lebih dalam mengenai inovasi apa saja yang dilakukan IOM untuk mengomunikasikan isu peretasan dan pencurian data kepada stafnya,

1.2. Rumusan Masalah

Seiring berkembangnya zaman, teknologi informasi dan komunikasi telah menjadi bagian penting bagi keberlangsungan organisasi. Walaupun keberadaan teknologi informasi dan komunikasi telah membawa dampak positif, namun dapat juga membawa risiko bagi organisasi. Risiko tersebut adalah peretasan dan pencurian data yang dilakukan oleh *hackers*.

IOM memiliki tanggung jawab untuk menjaga privasi dan keamanan data para imigran, donatur, pemerintah, dan pihak swasta yang merupakan *stakeholders*nya. Di tengah berbagai ancaman upaya peretasan dan pencurian data yang sering diterima, IOM melakukan program komunikasi internal untuk mengedukasi stafnya. IOM ingin stafnya memiliki pemahaman mendalam tentang cara mencegah peretasan dan pencurian data. Hal ini dilakukan karena walaupun ancamannya berasal dari luar organisasi, namun yang secara tidak sadar memberikan akses kepada para *hackers* ini adalah staf internal IOM sendiri.

Keberhasilan dan inovasi IOM dalam menciptakan program komunikasi internal ini menjadi daya tarik penulis untuk meneliti strategi perencanaannya dalam meningkatkan pengetahuan staf tentang pencegahan peretasan dan pencurian data.

1.3. Pertanyaan Penelitian

Berdasarkan rumusan masalah tersebut, pertanyaan dari penelitian ini adalah bagaimana strategi perencanaan program komunikasi internal IOM dalam mencegah peretasan dan pencurian data organisasi?

1.4.Tujuan Penelitian

Berdasarkan pertanyaan yang telah dirumuskan, tujuan dari penelitian ini adalah menganalisis strategi perencanaan program komunikasi internal IOM dalam mencegah peretasan dan pencurian data organisasi.

1.5. Kegunaan Penelitian

1.5.1 Kegunaan Akademis

Secara akademis, penelitian ini diharapkan dapat memberikan masukan yang bermanfaat bagi pengembangan ilmu komunikasi, terutama yang berkaitan dengan strategi perencanaan program komunikasi internal.

Kegunaan Praktis

Penelitian ini diharapkan dapat memberikan manfaat kepada IOM mengenai strategi perencanaan program komunikasi internal. Temuan-temuan dari penelitian ini akan berguna untuk memberikan masukan positif yang bisa digunakan IOM untuk meningkatkan kualitas program komunikasi internalnya dalam mengedukasi para staf. Penelitian ini juga diharapkan dapat menginspirasi organisasi, lembaga, dan perusahaan di luar sana untuk membuat program komunikasi yang dapat mengedukasi anggotanya mengenai dampak negatif yang datang dari teknologi informasi dan komunikasi, serta cara pencegahannya.

1.6. Keterbatasan Penelitian

Penelitian ini memiliki dua keterbatasan. Keterbatasan pertama terkait dengan waktu dan lokasi. IOM adalah organisasi internasional yang berada di luar negeri. Penelitian tidak dapat dilakukan secara langsung, melainkan melalui *video call*. Perbedaan jarak dan waktu yang cukup jauh membuat penulis harus menyesuaikan jadwal dengan ketersediaan partisipan sesuai dengan waktu setempatnya. Keterbatasan kedua terkait dengan data sekunder. Ada data-data organisasi yang dapat mendukung penelitian, namun bersifat konfidensial sehingga tidak dapat dicantumkan dalam karya tulisan ini.