BAB 2

TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Penggunaan HAIS-Q untuk mengukur *Information Security Awareness* telah dilakukan dalam beberapa penelitian dengan menggunakan metodologi yang berbeda-beda. Pattinson, Butavicius, Parsons, Mc Cormac, dan Jerram menggunakan metodologi Repertory Grid Technique (RGT) dengan dua puluh lima orang siswa sebagai sampel untuk mengetahui perilaku mereka terhadap keamanan informasi.[8] Pada tahun 2017, Parson juga menguji apakah HAIS-Q merupakan instrumen yang efektif dan valid jika digunakan untuk mengukur ISA dalam studi lanjutan.[1] Parson, dkk juga meneliti apakah hubungan antar budaya mempengaruhi keamanan informasi, hasil yang didapat menunjukkan nilai alpha cronbach diatas .80.

Pada tahun 2018, Cindana juga menggunakan HAIS-Q dalam penelitiannya dengan objek Perusahaan XYZ. Cindana menggunakan skala Kruger untuk mengukur ISA, ia juga menggunakan skor dengan nilai yang berbeda untuk menentukan kesimpulan yang didapat dari pengukuran pada skala Kruger yang ia gunakan. Hasil yang didapat Perusahaan XYZ sudah baik dalam menjaga ISA tetapi perlu adanya peningkatan fokus area pada penggunaan internet yang berpotensi merugikan. [9]

Pada tahun 2020, Zulfia dkk melakukan penelitian yang menggunakan HAIS-Q dengan sampel karyawan PT PQS. Mereka menggunakan skala Kruger menyusun rekomendasi menggunakan metode deskriptif. Hasil penelitian tersebut menunjukkan nilai alpha cornbach dari pengetahuan, sikap dan perilaku karyawan PT PQS diatas .80 atau bisa dibilang karyawan PT PQS cukup memiliki ISA yang baik. [6] Penelitian Safa dan Von sebelumnya juga menunjukkan bahwa kesadaran keamanan informasi karyawan (ISA) sangat penting dalam mengurangi risiko yang terkait dengan pelanggaran keamanan informasi. [10]

Pada penelitiannya Cormac dkk menunjukkan bahwa HAIS-Q dapat diandalkan secara eksternal dan internal. HAIS-Q merupakan alat ukur kesadaran keamanan informasi yang andal dan memungkinkan perusahaan untuk menilai keefektifan strategi keamanan informasi dari waktu ke waktu.[11]

Tahun 2019 Hwang dkk melakukan pengujian kepada 1198 karyawan organisasi dari berbagai industri menggunakan *Social Learning Teory* (SLT) untuk mengetahui bagaimana

pengalaman dan pengetahuan terkait keamanan informasi yang terjadi ditempat kerja. Dan mereka mendapatkan hasil bahwa beberapa faktor mempengaruhi keamanan informasi berdampak positif terhadap kesadaran keamanan informasi karyawan terhadap pendidikan, kebijakan, visibilitas keamanan dan partisipasi manajemen. Partisipasi keamanan manajerial memiliki hubungan terkuat dengan kesadaran karyawan dan juga memperkuat faktor organisasi dalam mempertahankan keamanan informasi. [7]

2.2. Dasar Teori

2.2.1 Definisi *Information Security Awareness* (ISA)

Information Security Awareness atau yang biasa disebut kesadaran keamanan informasi didefinisikan sebagai fokus perhatian pengguna terhadap keamanan, dengan tujuan untuk membantu individu dalam mengenali masalah keamanan dan dapat merespon masalah tersebut dengan tepat. ISA tidak semata-mata tentang pelatihan, melainkan tentang penerimaan informasi secara individu untuk membuat keputusan dengan lebih baik. ISA secara khusus dikonseptualisasikan sebagai kesadaran individu tentang peran dan tanggung jawab mereka mengenai keamanan informasi tersebut.

Information Security Awareness terfokus dalam dua aspek yaitu; Pertama, batasan seberapa jauh karyawan memahami perilaku keamanan informasi, yang didasarkan pada aturan, kebijakan dan pedoman organisasi terkait dengan keamanan informasi. Dan yang kedua, seberapa jauh karyawan berkomitmen dan berperilaku dalam *best practice*, sesuai dengan aturan, kebijakan dan pedoman organisasi terkait dengan keamanan informasi. ISA berfokus pada sejauh mana pemahaman individu terkait dengan kepentingan dan maksud kebijakan, aturan dan pedoman, serta perilaku mereka terhadap keamanan informasi. Definisi ini disesuaikan dengan dasar utama HAIS-Q yaitu *Knowledge - Attitude - Behavior* (KAB). Nantinya dari model KAB tersebut dapat dilihat apakah terdapat peningkatan tingkat pengetahuan karyawan tentang kebijakan dan prosedur keamanan dalam organisasi, sikap mereka terhadap kebijakan dan prosedur keamanan informasi, dan perilaku mereka terhadap keamanan informasi itu sendiri.

2.2.2 Pengukuran *Information Security Awareness* (ISA)

Beberapa penelitian telah melakukan pengukuran terhadap information security awareness. Seperti Hong Chang dalam tesisnya yang berjudul “Information Security Awareness Level of TAFE South Australia Employees” ia mengukur ISA dengan mengukur pengetahuan dan perilaku karyawan terhadap aspek-aspek keamanan informasi. Pengukuran

dilakukan secara sederhana berdasarkan persentase jawaban responden. Metode ini mengadopsi metode yang sebelumnya telah dilakukan oleh Kruger dan Kearney. [12]

Selain HAIS-Q, ada juga metode pengukuran ISA yaitu, User Information Security Awareness Questionnaire (UISAQ) yang diterapkan pada penelitian yang dilakukan oleh Galba dkk[13]. UISAQ terdiri dari 33 skala item yang berisikan perilaku dan pengetahuan serta kesadaran yang berpotensi beresiko. Menurut Galba dkk, secara keseluruhan keamanan informasi dipengaruhi oleh faktor kesadaran, pengetahuan dan perilaku dalam menggunakan internet.

Egelman dan Peer juga menyatakan bahwa tidak ada alat ukur standar untuk mengukur perilaku pengguna dalam menjaga keamanan informasi. Mereka juga telah mengembangkan Security Behavior Intentions Scale (SeBIS) yang berfokus pada kepatuhan karyawan terhadap keamanan perangkat komputer yang mereka gunakan seperti kesadaran dalam menjaga keamanan, pembuatan kata sandi dan pembaharuan.[14]

Selain itu pada tahun 2016, Ög˘ütçü dkk melakukan penelitian untuk menyelidiki perilaku beresiko yang dapat mengancam keamanan informasi. Mereka menggunakan *four scales of measurement* yang bergantung pada data yang terkumpul pada saat survey dilakukan. Upaya pengukuran ISA berada pada tahap awal pengembangan, dengan melakukan beberapa penilaian validitas dan reliabilitas.[15]

2.2.3 Human Aspects of Information Security Awareness Questionnaire (HAIS-Q)

Instrumen ini menggunakan rekomendasi McGuire (1969) dimana pengetahuan harus selalu diperhatikan terutama pengetahuan tentang kebijakan dan prosedur.[16] HAIS-Q dirancang untuk menggambarkan bidang keamanan informasi yang relevan dengan karyawan dan pengguna komputer yang rentan terhadap kegagalan keamanan informasi. *Human Aspects of Information Security Questionnaire* merupakan skala yang mengukur ISA yang mencakup 63 item sub-area yang dikategorisasikan menjadi 7 fokus area, yaitu manajemen *password*, pemakaian *email*, pemakaian internet, pemakaian social media, pemakaian perangkat seluler, penanganan informasi, dan pelaporan insiden. Setiap satu sub-area dinilai atau diukur melalui pengetahuan, sikap dan perilaku. Misalnya, dalam area fokus pengelolaan *password*, pernyataan spesifik tersebut meliputi:

- Pengetahuan : "Saya diizinkan untuk membagikan sandi kerja saya dengan rekan kerja"

- Sikap : "Tidak baik membagikan sandi kantor saya, meskipun rekan kerja saya yang memintanya"
- Perilaku: "Saya membagikan sandi kerja saya dengan rekan kerja"

Pengetahuan, sikap dan perilaku digunakan untuk menjaga keseimbangan antara ukuran spesifik area yang paling penting dan kebutuhan praktis untuk membatasi kuesioner. Sub-area yang ada pada HAIS-Q lebih spesifik dibandingkan dengan metode pengukuran kesadaran keamanan informasi lainnya dan cenderung mengukur keamanan informasi dalam hal yang sangat umum.