

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pelanggaran keamanan siber baru-baru ini telah menarik banyak perhatian organisasi untuk mengambil langkah-langkah yang tepat untuk mengamankan data, bisnis, dan untuk mengembangkan kebijakan siber yang efektif (Tjoa et al., 2016). Serangan siber secara umum, telah meningkat pada tingkat yang mengkhawatirkan dengan satu kasus yang terjadi setiap 39 detik (Washo, 2021). *Cybersecurity Ventures* memperkirakan biaya kejahatan dunia maya secara global akan terus meningkat 15 persen per tahun selama lima tahun ke depan, mencapai 10,5 triliun USD pada tahun 2025, naik dari 3 triliun USD pada tahun 2015 (Morgan, 2020).

Tren kejahatan siber di Indonesia pada tahun 2019 menempati urutan pertama dari tahun-tahun sebelumnya (Patrolisiber, 2019). Badan Siber dan Sandi Negara (BSSN) melaporkan 290,3 juta kasus serangan siber pada 2019 yang menyebabkan kerugian sebesar 34,2 miliar di Indonesia. Angka kasus tersebut secara signifikan meningkat jika dibandingkan dengan 232,4 juta kasus pada tahun sebelumnya. Sama halnya dengan Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim), yang melihat adanya peningkatan laporan kejahatan siber. Pada tahun 2019, 4.586 laporan polisi diajukan melalui Patrolisiber, laman website Bareskrim untuk melaporkan kejahatan siber. Sebuah peningkatan dari 4.360 laporan pada 2018 (Patrolisiber, 2020).

Pada kuartal pertama tahun 2020, Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa serangan siber yang terjadi di Indonesia mencapai 88,4 juta (Mutia, 2020). Puncak serangan terjadi pada 12 Maret 2020 dengan total serangan

mencapai 3,3 juta serangan/hari, bahkan interpol melakukan survei serangan siber terkait Covid-19 pada bulan Agustus 2020 yang mengungkapkan 59% serangan siber secara global. Berkaitan dengan hal tersebut dibutuhkan kemampuan dalam berlingkungan dan bertahan terhadap serangan siber yang biasa di sebut dengan *Cyber security*. *Cyber security* tidak hanya berhubungan dengan persoalan teknis seperti *hardware* dan *software* yang mencakup sistem jaringan informasi tetapi juga berhubungan dengan perilaku individual untuk menjaga *cyber security* (Safitri et al., 2020; Hidayah, 2020). Manusia bagaimanapun dianggap sebagai elemen terlemah dalam keamanan suatu sistem jaringan komputer (Mashiane & Kritzing, 2019). Masyarakat perlu untuk memahami perilaku terhadap teknologi keamanan atau *cyber security behavior* (Kovacevic et al., 2020). *Cyber security behavior* didefinisikan sebagai tindakan individu, reaksi, tingkah laku, dan perilaku umum dalam dunia siber (Olivier dan Chan, 2019)

Penelitian ini menggunakan variabel utama dalam perilaku keamanan siber dengan menggunakan perspektif *Health Belief Model* (HBM). Perspektif *Health Belief Model* (HBM) merupakan model konseptual yang biasa digunakan untuk menjelaskan perilaku kesehatan (Anwar et al., 2017), tetapi perspektif ini juga dianggap dapat menjelaskan perilaku keamanan siber karena model tersebut menunjukkan bahwa perilaku individu ditentukan oleh persepsi ancaman dan pertimbangan perilaku untuk mengatasi ancaman tersebut (Ng et al., 2009). Dalam preseptif HBM desain ini mengacu pada risiko subjektif dari tertularnya suatu kondisi (Ng et al., 2009). Menurut Rosenstock (1966), konsep pokok HBM terdiri

dari 6 komponen, yaitu persepsi kerentanan, persepsi keparahan, persepsi efikasi respon, persepsi hambatan, efikasi diri dan isyarat untuk bertindak.

Dalam konteks ini persepsi kerentanan yang dirasakan mengacu pada kemungkinan individu untuk percaya bahwa *computer* atau *handphone* mereka dapat terinfeksi virus atau diretas. Fatokun et al (2019) mengungkapkan individu yang teratur memanfaatkan internet secara eksploratif cenderung merasakan kerentanan terhadap keamanan siber. Keparahannya yang dirasakan berkaitan dengan keyakinan tentang keseriusan konsekuensi yang dihasilkan dari kondisi ini yang mengacu pada tingkat pemikiran tentang ancaman dan kesulitan yang diyakini akan muncul dari kondisi tersebut (Dodel & Mesch, 2019). Dalam menangani insiden keamanan siber, individu sering kali merasakan hambatan yang dapat mempengaruhi niat untuk mempraktikkan perilaku keamanan siber (Claar & Johnson, 2012).

Efikasi diri maupun efikasi respon dibutuhkan untuk meyakinkan individu dalam mengadopsi tindakan keamanan siber. Menurut Siponen et al (2014) menyebutkan bahwa efikasi diri memiliki dampak signifikan terhadap perilaku keamanan siber. Efikasi Diri mengacu pada penilaian individu tentang kemampuan mereka untuk melakukan tindakan penanggulangan keamanan siber dan dianggap sebagai kemampuan untuk mengatasi ancaman keamanan siber. Sedangkan efikasi respons mengacu pada sejauh mana individu percaya bahwa tanggapan yang direkomendasikan akan secara efektif mengurangi tingkat ancaman siber bagi mereka dan memiliki dampak signifikan terhadap perilaku keamanan informasi (Li et al., 2019).

Penelitian yang dilakukan oleh Ng et al (2009) dan Li et al (2019) mengatakan bahwa isyarat untuk bertindak dapat memotivasi individu untuk terlibat dalam perilaku keamanan informasi yang protektif. Hal ini mengacu pada pengetahuan individu atau informasi yang diperoleh dari sumber yang dapat dipercaya tentang penyebaran virus komputer, kerentanan komputer, atau aktivitas mencurigakan yang dapat menyebabkan serangan siber. Misalnya, seseorang lebih mungkin untuk menginstal perangkat lunak anti-virus jika melihat laporan berita tentang virus komputer menyebar di internet.

Penelitian ini juga menambahkan faktor *sensation seeking* sebagai prediktor selain prediktor-prediktor dalam HBM. Menurut hasil riset Kennison & Chan-Tin (2020) *sensation seeking* memiliki resiko lebih tinggi terkait keamanan siber dan menyumbang sekitar 35%. Individu dengan dorongan mencari sensasi cenderung memandang resiko sebagai suatu harga yang harus dibayar atau ditebus apabila ingin memperoleh *reward* tanpa melihat kesetaraan akan resiko yang diambil. Hal ini dilakukan semata-mata untuk meningkatkan perasaan sensasional, sehingga biasanya faktor pertimbangan secara rasional cenderung di abaikan, yang berpotensi membuat individu tersebut rentan terhadap keamanan siber (Levenson, 1990).

1.2 Rumusan masalah

Apakah terdapat hubungan antara perspektif HBM (kerentanan yang dirasakan, keparahan yang dirasakan, hambatan, efikasi respon, efikasi diri, isyarat untuk bertindak) dan *sensation seeking* terhadap perilaku keamanan siber.

1.3 Tujuan Penelitian

1.3.1 Tujuan Umum

Menganalisis kesadaran dan kewaspadaan pengguna media sosial terkait perilaku keamanan siber.

1.3.2 Tujuan Khusus

Untuk mengetahui hubungan perspektif HBM (kerentanan yang dirasakan, keparahan yang dirasakan, hambatan yang dirasakan, efikasi respon, efikasi diri, isyarat untuk bertindak) dan *sensation seeking* terhadap perilaku keamanan siber.

1.4 Manfaat Penelitian

Dengan dilaksanakannya penelitian ini, diharapkan dapat membawa manfaat baik manfaat teoritis maupun manfaat praktis, yaitu:

1.4.1 Manfaat Teoritis

Dapat menjadi acuan dalam melakukan penelitian selanjutnya, dan bermanfaat bagi para pembaca khususnya masyarakat dalam mempraktikkan keamanan siber.

1.4.2 Manfaat Praktis

1. Hasil penelitian ini dapat digunakan sebagai dasar dalam penelitian pada bidang perilaku keamanan siber.
2. Penelitian ini dapat digunakan dalam usaha penelusuran penyebab perilaku keamanan siber yang beresiko.
3. Badan Siber dan Sandi Negara (BSSN) dapat menggunakan penelitian ini sebagai acuan dalam penyusunan kebijakan dalam menangani permasalahan keamanan siber di Indonesia.