202210050311086
Fila Dwi Agustin
Prodi Ilmu Pemerintahan

BAB II
TINJAUAN PUSTAKA

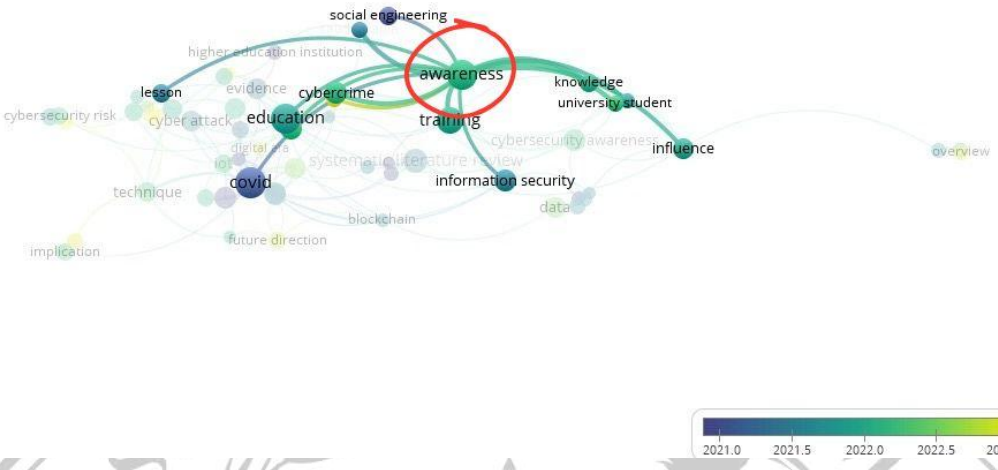
2.1 Penelitian Terdahulu

Dalam analisis bibliometrix, network visualization map dibawah ini menunjukkan bahwa kata "*Awareness*" memiliki posisi sentral dan terhubung dengan istilah lain seperti training, education, dan infromation security. Hal ini menandakan bahwa kesadaran keamanan merupakan fokus utama dalam penelitian terkait keamanan siber. Relevansinya dengan judul penelitian "Pengaruh Program Security Awareness dan Kebijakan Keamanan Informasi terhadap Budaya Keamanan Siber" terletak pada peran penting security awareness dalam membentuk perilaku aman pegawai dan memperkuat budaya keamanan di lingkungan organisasi.

Gambar 2.1 Network Visualization Map

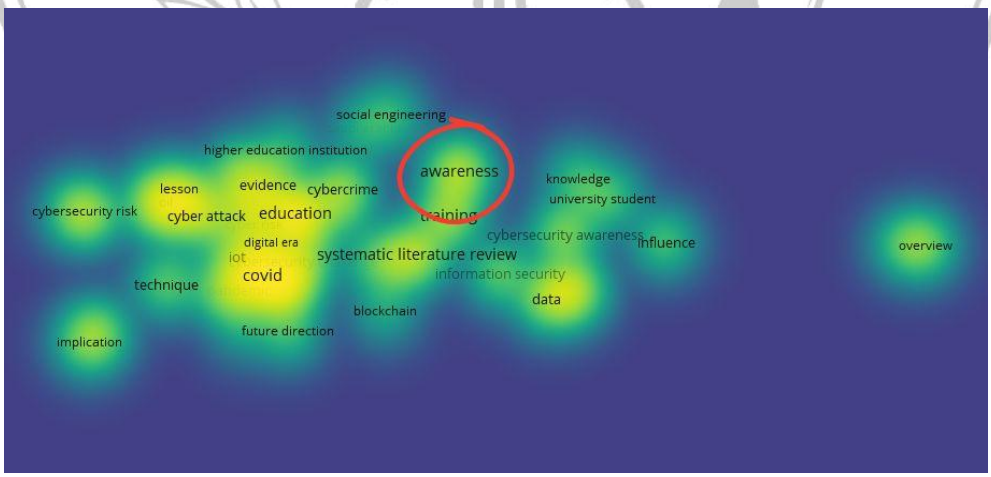
Pada gambar selanjutnya Overlay Visualization Map memperlihatkan peta keterkaitan topik penelitian berdasarkan waktu, dimana kata "Awareness" yang dilingkari merah menjadi pusat utama dan menunjukkan peningkatan perhatian dari tahun 2021 hingga 2023. Sehingga topik mengenai awareness masih sangat relevan untuk di teliti di tahun 2025. Hubungannya dengan istilah seperti training, education, dan information security menggambarkan bahwa kesadaran keamanan siber semakin dipandang penting dalam membangun prilaku aman digital.

Gambar 2.2 Overlay Visualization Map



Selanjutnya, pada density visualization map yang dihasilkan dari analisis bibliometrik menggunakan VOSviewer. Dalam peta ini, warna menunjukkan tingkat kepadatan atau frekuensi kemunculan suatu kata kunci dalam publikasi ilmiah. Kata "Awareness" yang dilingkari merah tampak berada di area berwarna paling terang (kuning cerah), menandakan bahwa istilah ini paling sering muncul dan menjadi pusat kajian dalam bidang keamanan siber. Hal ini menunjukkan bahwa topik security awareness memiliki pengaruh besar dan menjadi fokus utama dalam penelitian terkini.

Gambar 2.3 Density Visualization Map



Skripsi ini memiliki keunggulan daripada penelitian-penelitian yang sudah ada karena tidak hanya meneliti pengaruh program security awareness,

tetapi juga memasukkan peran kebijakan keamanan informasi dalam membangun budaya keamanan siber di kalangan pegawai Kementerian Komunikasi dan Digital republik Indonesia. Berbeda dengan penelitian-penelitian terdahulu yang umumnya hanya fokus pada security awareness atau budaya keamanan siber secara umum, skripsi ini menggabungkan kedua aspek tersebut. Oleh karena itu, penelitian ini mengisi kekurangan dari studi-studi sebelumnya dan memberikan kontribusi signifikan dalam pengembangan strategi keamanan informasi yang lebih menyeluruh di sektor pemerintahan.

Terdapat berbagai sumber ilmiah yang menyediakan penelitian pendahuluan, yaitu kajian yang telah dilakukan oleh peneliti lain dan mungkin ditemukan pada sumber, antara lain jurnal penelitian, tesis, disertasi, dan tesis lainnya. Berdasarkan penelitian peneliti, terdapat beberapa temuan penelitian yang berkaitan dengan peneliti ini. Berbagai penelitian sebagai berikut:

Tabel 2.1 Penelitian Terdahulu

No	Penulis	Judul	Variabel dan Model	Metode yang digunakan	Hasil
1.	Botagoz Khamzina, Nabuova Roza, Gulsara Zhussupbekova, Karlygash Shaizhanova, Aiganym Aten, Baikulova Aigerim	Determination of Cyber Security Issues and Awareness Training for University Students	Kesadaran keamanan siber dan kesadaran serangan siber sebelum dan sesudah pelatihan	Kuantitatif	Kesadaran keamanan siber mahasiswa meningkat signifikan setelah mengikuti pelatihan online. Mahasiswa laki-laki menunjukkan tingkat kesadaran lebih tinggi dibanding

No	Penulis	Judul	Variabel dan Model	Metode yang digunakan	Hasil
	Meirkhanovna				perempuan sebelum pelatihan.
2.	Talal Alharbi & Asifa Tassaddiq	Assessment of Cybersecurity Awareness among Students of Majmaah University	Kesadaran keamanan siber mahasiswa (email, virus komputer, phishing, iklan palsu, popup, dll.)	Kuantitatif	Kesadaran keamanan siber mahasiswa masih rendah, banyak yang tidak memahami firewall, 2FA, atau bahaya software gratis. Perlu program pelatihan menyeluruh untuk meningkatkan kesadaran.
3.	Peter Dornheim & Ruediger Zarnekow	Determining Cybersecurity Culture Maturity and Deriving Verifiable Improvement Measures	Maturitas budaya keamanan siber (akuntabilitas, komitmen, efektivitas kebijakan, persepsi penggunaan informasi, dukungan manajemen)	Kuantitatif	Survei pertama menunjukkan kelemahan pada akuntabilitas, komitmen, efektivitas kebijakan; setelah tindakan perbaikan, survei kedua menunjukkan peningkatan signifikan pada dimensi tersebut.

No	Penulis	Judul	Variabel dan Model	Metode yang digunakan	Hasil
4.	Mohammed A. Alqahtani	Factors Affecting Cybersecurity Awareness among University Students	Keamanan kata sandi, keamanan browser, aktivitas media sosial	Kuantitatif	Ketiga variabel (keamanan kata sandi, keamanan browser, aktivitas media sosial) berpengaruh signifikan terhadap kesadaran keamanan siber mahasiswa.
5.	Adamu A. Garba, Maheyzah Md. Siraj, Siti Hajar Othman & M.A. Musa	A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach	Tingkat kesadaran keamanan siber mahasiswa (pengetahuan, privasi, kepercayaan, manajemen kata sandi, dan keinginan belajar)	Kuantitatif	Kesadaran mahasiswa berada pada tingkat sedang, sebagian besar tidak memahami phishing, 2FA, dan manajemen kata sandi. Mahasiswa perempuan lebih rentan menjadi korban serangan siber. 95% responden ingin mempelajari lebih lanjut tentang keamanan siber.

Sumber: Data di Olah dari Hasil Wawancara Oleh Peneliti

2.2 Kerangka Teori

2.2.1 Implementasi Program Security Awareness dalam Perspektif Teori George C. Edward III

Implementasi kebijakan merupakan tahap penting dalam proses kebijakan publik karena keberhasilan suatu kebijakan tidak hanya ditentukan oleh kualitas perumusannya, tetapi juga oleh bagaimana kebijakan tersebut dilaksanakan. Menurut George C. Edward III, implementasi kebijakan adalah proses pelaksanaan keputusan atau kebijakan yang telah ditetapkan oleh pembuat kebijakan untuk mencapai tujuan yang diinginkan. Keberhasilan implementasi kebijakan dipengaruhi oleh empat faktor utama, yaitu komunikasi, sumber daya, disposisi, dan struktur birokrasi.

Dalam penelitian ini, Program Security Awareness dipandang sebagai suatu program yang diimplementasikan oleh Kementerian Komunikasi dan Digital untuk meningkatkan pengetahuan keamanan siber pegawai. Oleh karena itu, teori implementasi kebijakan Edward III digunakan untuk menjelaskan bagaimana pelaksanaan Program Security Awareness dapat memengaruhi tingkat pengetahuan keamanan siber pegawai.

1. Komunikasi (Communication)

Komunikasi merupakan proses penyampaian informasi mengenai kebijakan atau program kepada pihak yang melaksanakan maupun pihak yang menjadi sasaran program. Komunikasi yang efektif diperlukan agar tujuan, isi, dan prosedur program dapat dipahami dengan baik oleh seluruh pegawai. Menurut Edward III, komunikasi yang baik ditandai dengan adanya transmisi informasi yang tepat, kejelasan pesan, dan konsistensi informasi yang disampaikan.

Dalam Program Security Awareness, komunikasi diwujudkan melalui sosialisasi, pelatihan, seminar, webinar, maupun penyampaian informasi terkait keamanan siber kepada pegawai. Semakin jelas dan konsisten informasi yang diterima pegawai, maka semakin besar

kemungkinan pegawai memahami materi keamanan siber yang diberikan.

2. Sumber Daya (Resources)

Sumber daya merupakan faktor yang mendukung keberhasilan pelaksanaan suatu program. Meskipun komunikasi telah berjalan dengan baik, implementasi program tidak akan berhasil apabila tidak didukung oleh sumber daya yang memadai. Edward III menjelaskan bahwa sumber daya meliputi sumber daya manusia, informasi, kewenangan, serta fasilitas pendukung.

Dalam konteks Program Security Awareness, sumber daya dapat berupa kompetensi instruktur atau narasumber, materi pelatihan, media pembelajaran, sarana dan prasarana teknologi informasi, serta dukungan anggaran yang memadai. Ketersediaan sumber daya tersebut akan membantu pegawai memperoleh pengetahuan keamanan siber secara optimal.

3. Disposisi (Disposition)

Disposisi merupakan sikap, komitmen, dan kemauan para pelaksana maupun peserta program dalam menjalankan kebijakan yang telah ditetapkan. Menurut Edward III, keberhasilan implementasi sangat dipengaruhi oleh kesediaan individu untuk menerima dan melaksanakan kebijakan sesuai dengan tujuan yang telah ditetapkan.

Dalam Program Security Awareness, disposisi tercermin dari kemauan pegawai untuk mengikuti pelatihan, kesungguhan dalam memahami materi yang diberikan, serta komitmen untuk menerapkan praktik keamanan siber dalam aktivitas kerja sehari-hari. Semakin tinggi komitmen pegawai terhadap program, maka semakin besar peluang peningkatan pengetahuan keamanan siber.

4. Struktur Birokrasi (Bureaucratic Structure)

Struktur birokrasi merupakan mekanisme organisasi yang mengatur pelaksanaan program agar berjalan secara efektif dan terkoordinasi. Edward III menjelaskan bahwa struktur birokrasi berkaitan dengan

pembagian tugas, prosedur kerja, koordinasi antarunit, serta standar operasional prosedur (SOP).

Dalam Program Security Awareness, struktur birokrasi diwujudkan melalui adanya pedoman pelaksanaan program, pembagian tanggung jawab yang jelas, mekanisme koordinasi antarunit kerja, serta evaluasi pelaksanaan program secara berkala. Struktur birokrasi yang baik akan mendukung kelancaran pelaksanaan program dan pencapaian tujuan yang telah ditetapkan.

2.2.2 Pengetahuan Keamanan Siber

Pengetahuan keamanan siber merupakan tingkat pemahaman individu mengenai berbagai ancaman keamanan informasi, cara melindungi data dan sistem informasi, serta tindakan yang harus dilakukan untuk mencegah maupun menangani insiden keamanan siber. Pengetahuan keamanan siber menjadi salah satu faktor penting dalam upaya perlindungan informasi organisasi karena manusia sering kali menjadi sasaran utama berbagai serangan siber.

Dalam penelitian ini, pengetahuan keamanan siber diukur melalui pemahaman pegawai mengenai ancaman siber, perlindungan data dan akun, penggunaan sistem yang aman, serta penanganan insiden keamanan siber. Semakin tinggi tingkat pengetahuan pegawai mengenai keamanan siber, maka semakin kecil risiko terjadinya kesalahan manusia yang dapat menyebabkan kebocoran atau gangguan keamanan informasi organisasi.

2.2.3 Hubungan Program Security Awareness dengan Pengetahuan Keamanan Siber

Program Security Awareness merupakan salah satu upaya organisasi untuk meningkatkan pemahaman pegawai mengenai keamanan informasi dan ancaman siber. Melalui berbagai kegiatan edukasi, pelatihan, dan sosialisasi, pegawai memperoleh pengetahuan mengenai cara mengidentifikasi ancaman, melindungi data,

menggunakan teknologi secara aman, serta merespons insiden keamanan siber.

Berdasarkan teori implementasi kebijakan Edward III, keberhasilan Program Security Awareness dipengaruhi oleh komunikasi yang efektif, sumber daya yang memadai, disposisi peserta yang positif, dan struktur birokrasi yang mendukung. Apabila keempat faktor tersebut berjalan dengan baik, maka pelaksanaan Program Security Awareness akan semakin efektif sehingga mampu meningkatkan pengetahuan keamanan siber pegawai.

Dengan demikian, dapat diasumsikan bahwa semakin baik implementasi Program Security Awareness, maka semakin tinggi pula tingkat pengetahuan keamanan siber pegawai di lingkungan Kementerian Komunikasi dan Digital Republik Indonesia.

2.2.4 Hipotesis

H_0: Program Security Awareness tidak berpengaruh signifikan terhadap pengetahuan keamanan siber pegawai di lingkungan Kementerian Komunikasi dan Digital Republik Indonesia.

H_1: Program Security Awareness berpengaruh signifikan terhadap pengetahuan keamanan siber pegawai di lingkungan Kementerian Komunikasi dan Digital Republik Indonesia.