JTRISTE, Vol.13, No.2, Oktober 2026, pp. 58~72
ISSN: **2355-3677 | e-ISSN : 2460-8548**

Ilusi Keamanan pada Security Operations Center (SOC): Kajian Literatur Sistematis tentang False Sense of Security dalam Mendukung Ketahanan Siber

Thata Apriatin[1*], Imam Riadi[2], Herman[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
Jl. Ahmad Yani (ringroad Selatan) Tamanan, Bangun Tapan, Bantul, Yogyakarta, Indonesia
e-mail: [1]2536083021@webmail.uad.ac.id,[2] imam.riadi@uad.ac.id,[3] hermankaha@uad.ac.id

Abstrak

Fenomena false sense of security dalam keamanan siber terjadi ketika individu atau organisasi merasa bahwa sistem telah berada dalam kondisi aman, meskipun perlindungan aktual belum tentu memadai. Kondisi ini menjadi semakin penting pada lingkungan Security Operations Center (SOC) modern yang banyak bergantung pada Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Threat Intelligence Platform, serta sistem pemantauan berbasis Artificial Intelligence (AI). Dalam praktik SOC, rasa aman yang semu dapat muncul ketika analis terlalu percaya pada dashboard, playbook, dan hasil deteksi otomatis tanpa melakukan validasi kontekstual yang memadai. Ketergantungan berlebihan terhadap teknologi tersebut berpotensi menimbulkan automation bias, alert fatigue, serta menurunkan kemampuan analis dalam mengenali anomali yang tidak langsung terdeteksi oleh sistem. Penelitian ini bertujuan mengidentifikasi faktor-faktor yang membentuk false sense of security pada operasional SOC, mengevaluasi strategi intervensi yang telah diteliti, serta menyusun sintesis konseptual mengenai hubungan antara faktor psikologis, otomatisasi berbasis AI, dan cyber resilience. Metode yang digunakan adalah Systematic Literature Review (SLR) dengan mengacu pada pedoman PRISMA 2020. Literatur diperoleh dari IEEE Xplore, Scopus, ACM Digital Library, ScienceDirect, dan Google Scholar menggunakan kombinasi kata kunci false sense of security, cybercomplacency, automation bias, Security Operations Center, dan cyber resilience. Dari proses seleksi diperoleh 27 artikel yang dianalisis menggunakan pendekatan thematic synthesis. Hasil kajian menunjukkan bahwa false sense of security pada SOC dipengaruhi oleh interaksi antara bias kognitif, kepercayaan berlebihan terhadap AI, alert fatigue, dan budaya organisasi yang terlalu berorientasi pada kepatuhan. Kajian ini berkontribusi dengan menempatkan false sense of security sebagai konstruk penghubung antara psikologi keamanan siber, praktik operasional SOC, dan cyber resilience, sehingga dapat menjadi dasar bagi pengembangan model empiris pada penelitian berikutnya.

Kata kunci: *False Sense of Security, Security Operations Center, Cybersecurity Psychology, Cyber Resilience, Artificial Intelligence.*

Abstract

False sense of security in cybersecurity occurs when individuals or organizations believe that their systems are secure, although the actual level of protection may not be sufficient. This issue is increasingly relevant in modern Security Operations Center (SOC) environments, where security operations rely heavily on Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Threat Intelligence Platforms, and Artificial Intelligence (AI)-driven monitoring systems. In SOC practice, a misleading sense of safety may emerge when analysts place excessive trust in dashboards, playbooks, and automated detection results without sufficient contextual validation. Such overreliance may contribute to automation bias, alert fatigue, and a decline in analysts' ability to recognize anomalies that are not directly detected by security tools. This study aims to identify the factors that shape false sense of security in SOC operations, evaluate existing intervention strategies, and

[*] Corresponding author : Thata Apriatin (2536083021@webmail.uad.ac.id)

Diterima : *Mei, 2026* ***Disetujui :*** *Juli, 2026* ***Dipublikasikan :*** *Oktober, 2026*

develop a conceptual synthesis of the relationship between psychological factors, AI-driven automation, and cyber resilience. This study employs a Systematic Literature Review (SLR) method based on the PRISMA 2020 guideline. Literature was collected from IEEE Xplore, Scopus, ACM Digital Library, ScienceDirect, and Google Scholar using keyword combinations related to false sense of security, cybercomplacency, automation bias, Security Operations Centre, and cyber resilience. The selection process resulted in 27 articles, which were analysed using a thematic synthesis approach. The findings indicate that false sense of security in SOC environments is shaped by the interaction between cognitive bias, excessive trust in AI, alert fatigue, and an organizational culture that is overly compliance-oriented. This review contributes by positioning false sense of security as a connecting construct between cybersecurity psychology, SOC operational practice, and cyber resilience, thereby providing a foundation for developing empirical models in future research.

Keywords: *False Sense of Security, Security Operations Center, Cybersecurity Psychology, Cyber Resilience, Artificial Intelligence.*

1. Pendahuluan

Keamanan siber selama ini sering dipandang sebagai persoalan teknis, yakni soal kekuatan enkripsi, ketepatan konfigurasi firewall, atau kecanggihan sistem deteksi intrusi yang dipasang pada infrastruktur. Pandangan tersebut tidak sepenuhnya keliru, tetapi cenderung mengesampingkan satu variabel yang dalam praktik justru paling sering menjadi titik kegagalan, yaitu manusia. Secara lebih spesifik, kegagalan keamanan lebih sering dipicu oleh keyakinan berlebih bahwa sistem yang dimiliki sudah cukup terlindungi daripada oleh ketidaktahuan terhadap ancaman.

Kondisi seperti itulah yang dalam literatur dikenal sebagai false sense of security atau ilusi keamanan. Konsep ini tidak menggambarkan individu atau organisasi yang sama sekali tidak memahami risiko, melainkan kondisi ketika ancaman sebenarnya diketahui, tetapi tingkat bahayanya dianggap tidak terlalu dekat atau tidak terlalu mendesak. Dalam konteks keamanan siber, pola ini berkaitan dengan cybercomplacency, yaitu kecenderungan untuk merasa cukup aman meskipun masih terdapat risiko yang belum sepenuhnya dikendalikan [1], [6]. Pada lingkungan Security Operations Center (SOC), bentuknya dapat terlihat ketika analis atau organisasi terlalu cepat merasa aman hanya karena dashboard SIEM tampak stabil, jumlah alert kritis menurun, atau laporan kepatuhan terlihat terpenuhi.

Dalam praktik SOC, kondisi aman tidak selalu berarti tidak ada serangan. Beberapa ancaman dapat berjalan perlahan, menggunakan kredensial yang sah, atau belum menghasilkan pola yang cukup kuat untuk terangkat sebagai alert prioritas tinggi. Karena itu, alert yang tampak rendah tidak seharusnya langsung dipahami sebagai risiko yang rendah. Validasi manual tetap diperlukan, misalnya dengan memeriksa riwayat aktivitas pengguna, perubahan konfigurasi, korelasi dengan threat intelligence, serta pola komunikasi jaringan yang tidak biasa. Tanpa proses tersebut, keputusan analis berisiko lebih banyak dipengaruhi oleh tampilan sistem dibandingkan oleh pemahaman terhadap konteks insiden yang sebenarnya. Sejumlah studi tentang SOC juga menunjukkan bahwa volume alert yang tinggi dan banyaknya false positive dapat menurunkan ketelitian analis dalam proses investigasi [28], [29], [30].

Tantangan ini semakin kompleks ketika SOC mulai mengandalkan AI-driven monitoring, automated detection, dan playbook SOAR. Teknologi tersebut memang membantu mempercepat triase dan mengurangi beban kerja, tetapi juga dapat menciptakan ketergantungan baru. Ketika analis terlalu sering menerima rekomendasi sistem tanpa mempertanyakannya kembali, ruang untuk berpikir kritis menjadi lebih sempit. Dalam literatur human factors, kecenderungan ini dikenal sebagai automation bias, yaitu kondisi ketika manusia terlalu mempercayai keluaran sistem otomatis, termasuk dalam situasi yang sebenarnya masih membutuhkan penilaian manual [38], [39], [40].

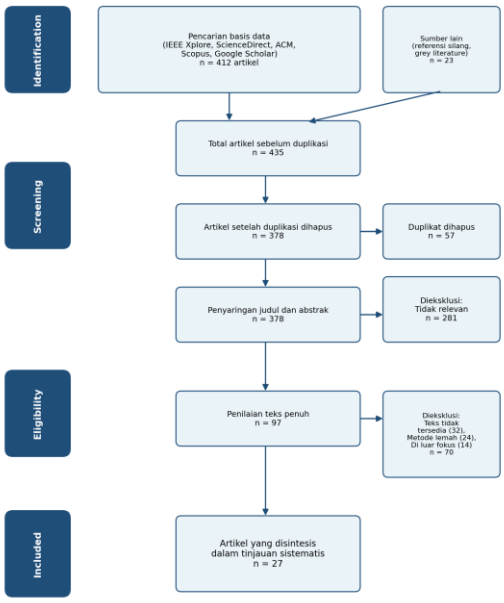
Karena itu, false sense of security pada SOC tidak dapat dipahami semata sebagai persoalan teknis. Dashboard yang terlihat hijau, alert yang tampak terkendali, dan dokumen kepatuhan yang lengkap memang penting, tetapi belum cukup untuk memastikan bahwa organisasi benar-benar aman. Keamanan siber tetap membutuhkan validasi kontekstual, pembacaan lintas sumber data, serta budaya kerja yang memberi ruang bagi analis untuk mempertanyakan hasil otomatisasi. Oleh karena itu, ilusi keamanan perlu dilihat sebagai persoalan psikologis, teknis, dan organisasional sekaligus [5], [24].

2. Metode Penelitian

Kajian ini menggunakan pendekatan systematic literature review (SLR) yang mengacu pada panduan PRISMA. Tujuan dari pendekatan ini adalah memetakan secara terstruktur literatur yang membahas false sense of security pada konteks keamanan siber, khususnya yang berkaitan dengan akar psikologis, strategi intervensi, dan ketahanan organisasi. Pencarian literatur dilakukan pada beberapa basis data utama, mencakup IEEE Xplore, ScienceDirect, ACM Digital Library, Scopus, dan Google Scholar, dengan rentang publikasi 1999 sampai dengan 2025 agar dapat menangkap baik karya seminal maupun perkembangan terbaru.

Kata kunci yang digunakan meliputi false sense of security, cybercomplacency, automation bias, alert fatigue, security awareness, optimism bias, security operations center (SOC), dan cyber resilience. Kombinasi kata kunci tersebut diterapkan menggunakan operator Boolean (AND, OR) untuk memperluas cakupan tanpa kehilangan ketepatan. Hasil pencarian awal kemudian disaring melalui beberapa tahap, yaitu pemeriksaan judul, pembacaan abstrak, dan penilaian kelayakan teks penuh. Alur lengkap proses seleksi literatur mengikuti panduan PRISMA seperti diperlihatkan pada Gambar 1.

Agar proses pencarian dapat ditelusuri ulang, string penelusuran disusun spesifik untuk tiap basis data dengan menyesuaikan sintaks masing-masing. Pada IEEE Xplore dan ACM Digital Library, penelusuran memakai kombinasi ("false sense of security" OR "cybercomplacency" OR "automation bias") AND ("security operations center" OR "SOC" OR "cyber resilience") yang diterapkan pada bidang judul, abstrak, dan kata kunci. Pada Scopus dan ScienceDirect, ekspresi serupa dijalankan melalui pola TITLE-ABS-KEY dengan penambahan ("alert fatigue" OR "security awareness" OR "optimism bias") sebagai perluasan, sedangkan Google Scholar digunakan untuk penelusuran teks bebas guna menangkap grey literature dan karya seminal yang mungkin tidak terindeks pada empat basis data lainnya. Rentang publikasi dibatasi pada 1999 hingga 2025, dengan pengecualian bagi rujukan teori dasar yang terbit lebih awal. Seluruh string, tanggal akses, dan jumlah rekaman yang ditemukan pada tiap basis data dicatat dalam lembar penelusuran sebagai dokumentasi pendukung, sehingga proses identifikasi dapat direplikasi dan angka pada diagram PRISMA dapat ditelusuri kembali ke sumbernya.



Gambar 1. Diagram Alur PRISMA Seleksi Literatur

Gambar 1 menggambarkan tahapan seleksi literatur yang ditempuh pada kajian ini. Tahap identifikasi menghasilkan total 412 artikel dari lima basis data utama serta 23 artikel tambahan yang diperoleh melalui penelusuran referensi silang dan grey literature, sehingga keseluruhan

kandidat awal berjumlah 435 artikel. Sebanyak 57 artikel duplikat kemudian dihapus pada tahap awal screening. Tahap penyaringan judul dan abstrak menyisihkan 281 artikel yang dinilai tidak relevan dengan fokus kajian. Tahap eligibility menilai 97 artikel dalam bentuk teks penuh, di mana 70 artikel selanjutnya dieksklusi karena teks penuh tidak tersedia, metodologinya lemah, atau substansinya berada di luar fokus kajian. Pada akhir proses, 27 artikel memenuhi seluruh kriteria dan dianalisis lebih lanjut pada tahap sintesis tematik. Kedua puluh tujuh artikel tersebut merupakan studi primer yang menjadi korpus analisis sistematis, sedangkan rujukan lain yang muncul dalam artikel ini berperan sebagai landasan teoretis, metodologis, dan kontekstual, sehingga jumlah entri pada daftar pustaka wajar melampaui jumlah studi primer yang diikutkan.

Tabel 1. Kriteria Inklusi dan Eksklusi Literatur

Kriteria Inklusi	Kriteria Eksklusi
Artikel peer-reviewed pada jurnal atau prosiding terindeks.	Artikel opini, blog, dan dokumen non-akademik tanpa proses peninjauan sejawat.
Publikasi pada rentang tahun 1999 hingga 2025.	Publikasi sebelum 1999 kecuali bersifat seminal seperti rujukan teori dasar.
Berbahasa Inggris atau Indonesia.	Berbahasa selain Inggris atau Indonesia.
Membahas aspek psikologis, perilaku, atau organisasional dari keamanan siber.	Hanya membahas aspek teknis tanpa singgungan dengan faktor manusia atau organisasi.
Memuat kerangka teori, hasil empiris, atau analisis kasus relevan.	Duplikasi publikasi dan artikel dengan teks penuh tidak tersedia.

Tabel 1 menyajikan kriteria seleksi yang digunakan untuk menjaga ketelitian dan ketelusuran proses review. Penerapan kriteria tersebut dilakukan secara berurutan, dimulai dari penyaringan otomatis melalui filter basis data hingga penilaian manual atas teks penuh. Pada tahap akhir, sebanyak dua puluh tujuh artikel dianggap memenuhi kriteria dan dimasukkan ke dalam analisis sintesis.

Analisis terhadap literatur dilakukan dengan teknik thematic synthesis. Setiap artikel dikodifikasi berdasarkan tema yang muncul, terutama tema akar psikologis, strategi intervensi, dan peran ketahanan siber. Tema-tema tersebut kemudian dikelompokkan menjadi pola yang lebih besar dan dibandingkan antarstudi untuk mengidentifikasi titik temu, kontradiksi, serta celah riset. Validitas hasil sintesis dijaga melalui pemeriksaan silang antar tim penulis dan dokumentasi audit trail terhadap setiap keputusan inklusi maupun eksklusi.

Ekstraksi data dilakukan menggunakan formulir terstruktur yang merekam identitas artikel, konteks studi, desain penelitian, konstruk psikologis atau organisasional yang diamati, jenis intervensi apabila ada, serta temuan utama yang relevan dengan ilusi keamanan. Formulir tersebut diisi oleh satu penulis dan diperiksa ulang oleh penulis lain untuk mengurangi bias penilaian. Perbedaan interpretasi diselesaikan melalui diskusi hingga tercapai kesepakatan, dan setiap keputusan dicatat pada lembar audit trail.

Penilaian kualitas metodologis dilakukan agar bobot temuan sepadan dengan kekuatan buktinya. Artikel empiris ditelaah berdasarkan kejelasan tujuan, ketepatan desain, kememadaian ukuran sampel, dan konsistensi antara data dan simpulan, sedangkan artikel konseptual dinilai dari kejelasan argumentasi serta keterhubungannya dengan literatur yang mapan. Studi dengan keterbatasan metodologis berat tetap dipertahankan bila memberi wawasan konseptual penting, tetapi klaimnya diposisikan sebagai indikatif dan bukan konklusif. Pendekatan bertingkat ini memungkinkan sintesis membedakan temuan yang telah diuji secara empiris dari proposisi yang masih bersifat teoretis.

3. Hasil Dan Pembahasan

3.1. Akar Psikologis False Sense of Security

False sense of security pada keamanan siber tidak muncul secara tiba-tiba. Fenomena ini terbentuk ketika persepsi aman lebih dominan dibandingkan penilaian kritis terhadap kondisi

keamanan yang sebenarnya. Di lingkungan SOC, persoalan ini menjadi lebih kompleks karena analis bekerja dalam lingkungan yang sangat bergantung pada dashboard, alert, indikator prioritas, dan sistem korelasi otomatis. Ketika semua indikator terlihat normal, rasa aman dapat terbentuk lebih cepat daripada proses validasi risiko yang seharusnya dilakukan.

Akar utama dari kondisi tersebut dapat dijelaskan melalui beberapa konsep psikologis. Prospect theory menjelaskan bahwa manusia tidak selalu menilai risiko secara rasional, terutama ketika menghadapi ancaman yang jarang terjadi tetapi berdampak besar [3], [47]. Dalam keamanan siber, pola ini terlihat ketika organisasi memahami bahwa serangan dapat terjadi, tetapi tetap merasa bahwa kemungkinannya kecil untuk menimpa sistem mereka. Optimism bias memperkuat kondisi tersebut karena individu cenderung merasa lebih mampu menghindari risiko dibandingkan pihak lain [4], [46]. Di SOC, bias ini dapat muncul dalam bentuk keyakinan bahwa sistem deteksi yang digunakan sudah cukup matang sehingga ancaman besar pasti akan terangkat sebagai alert.

Perbedaan antara keamanan objektif dan keamanan subjektif menjadi titik penting dalam memahami ilusi keamanan [5]. Keamanan objektif berkaitan dengan kondisi teknis yang dapat diuji, seperti konfigurasi, deteksi, kontrol akses, dan efektivitas respons. Sebaliknya, keamanan subjektif berkaitan dengan rasa aman yang terbentuk dari pengalaman, tampilan sistem, atau keyakinan terhadap prosedur yang berjalan. Masalah muncul ketika keamanan subjektif lebih kuat daripada bukti objektif. Dashboard SIEM yang terlihat hijau, jumlah alert yang menurun, atau laporan kepatuhan yang lengkap dapat membentuk rasa aman, meskipun belum tentu mencerminkan bahwa semua celah telah terkendali.

Dalam praktik SOC, cybercomplacency menjadi wujud perilaku dari rasa aman yang berlebihan. Analis atau organisasi tidak selalu mengabaikan risiko karena tidak tahu, tetapi karena menganggap risiko tersebut sudah cukup tertangani oleh sistem, prosedur, atau tim yang ada [1], [6]. Kondisi ini berbahaya karena mengurangi dorongan untuk melakukan pengecekan ulang. Alert dengan prioritas rendah dapat langsung dianggap tidak signifikan, padahal konteks tertentu seperti akses dari akun sah, perubahan perilaku pengguna, atau komunikasi jaringan yang tidak biasa tetap membutuhkan validasi manual.

Automation bias memperkuat masalah tersebut pada SOC modern. Semakin banyak proses keamanan dibantu oleh AI-driven monitoring, automated detection, dan playbook SOAR, semakin besar pula kemungkinan analis menerima keluaran sistem sebagai keputusan final. Padahal, otomatisasi seharusnya mendukung penilaian manusia, bukan menggantikannya sepenuhnya. Literatur human factors menyebut bahwa manusia cenderung terlalu mempercayai sistem otomatis ketika sistem tersebut tampak konsisten dan jarang salah [38], [39], [40]. Dalam SOC, pola ini dapat terlihat ketika analis lebih percaya pada severity yang diberikan sistem dibandingkan membaca konteks insiden secara mandiri.

Alert fatigue juga menjadi faktor yang sangat berpengaruh. Ketika analis menerima terlalu banyak notifikasi, terutama false positive, kemampuan untuk membedakan sinyal penting dari noise akan menurun [28], [29], [30]. Dalam kondisi kelelahan, keputusan sering kali dibuat berdasarkan kebiasaan dan kecepatan, bukan analisis mendalam. Akibatnya, proses investigasi menjadi lebih mekanis: alert dibuka, status diperiksa, indikator dilihat, lalu tiket ditutup. Jika pola ini berlangsung terus-menerus, SOC dapat terlihat aktif secara operasional tetapi kehilangan ketajaman analitis.

Pada akhirnya, false sense of security pada SOC merupakan hasil interaksi antara bias kognitif, kelelahan operasional, kepercayaan berlebih terhadap otomatisasi, dan budaya kerja yang terlalu percaya pada indikator formal. Yang menjadi persoalan bukan sekadar apakah teknologi keamanan bekerja; yang lebih menentukan adalah apakah manusia dan organisasi masih terbiasa mempertanyakan hasil yang diberikan teknologi tersebut.

Tabel 2. Ringkasan Teori Utama yang Membentuk Pemahaman False Sense of Security

No	Teori / Konsep	Kontribusi terhadap Pemahaman Ilusi Keamanan
1	Prospect Theory [3]	Menjelaskan distorsi sistematis dalam estimasi probabilitas, khususnya pada kejadian berpeluang kecil namun berdampak besar yang sejajar dengan ancaman siber.
2	Optimism Bias [4]	Memperlihatkan kecenderungan individu merasa lebih kebal terhadap risiko dibanding

		orang lain, dan bias ini tidak melemah meskipun pengetahuan teknis meningkat.
3	Keamanan Subjektif vs Objektif [5]	Memetakan celah antara kondisi keamanan aktual dan persepsi pengguna sebagai ruang tumbuhnya ilusi keamanan.
4	Cybercomplacency [6]	Menangkap dimensi perilaku dari kelalaian siber yang berakar pada pengetahuan adanya ancaman tanpa rasa keterhubungan personal terhadap risiko.
5	Protection Motivation Theory [8]	Memberi kerangka penilaian ancaman dan efikasi respons sebagai dua faktor yang menentukan munculnya motivasi proteksi.

Berdasarkan Tabel 2 di atas terlihat bahwa pemahaman atas false sense of security berdiri pada fondasi lintas disiplin yang mencakup ekonomi perilaku, psikologi kognitif, hingga ilmu informasi. Kelima kerangka tersebut tidak berdiri sendiri, tetapi saling mengisi. Prospect theory dan optimism bias menjelaskan asal usul distorsi penilaian risiko, sedangkan konsep keamanan subjektif dan cybercomplacency memberi nama pada bentuk-bentuk manifestasinya. Protection Motivation Theory kemudian menyatukan keduanya ke dalam model proses kognitif yang memprediksi apakah seseorang akan bertindak proteksi atau tidak.

Distorsi penilaian tersebut memperoleh bentuk yang khas ketika berhadapan dengan sistem otomatis. Literatur faktor manusia sejak lama menunjukkan bahwa operator cenderung terlalu mempercayai keluaran otomatis dan menurunkan kewaspadaan ketika sistem tampak andal, sebuah pola yang dikenal sebagai automation bias dan complacency [38], [39]. Kalibrasi kepercayaan terhadap otomatisasi karenanya menjadi persoalan inti, sebab kepercayaan yang tidak sepadan dengan keandalan aktual sistem justru melemahkan kinerja pengambilan keputusan [40]. Dalam operasional SOC, kecenderungan ini diperparah oleh volume alert yang sangat tinggi. Studi kualitatif terhadap analis memperlihatkan bahwa sebagian besar alert bersifat false positive sehingga proses validasi terasa melelahkan dan kepekaan terhadap anomali kritis menurun [28], [29]. Eksperimen pada konteks keputusan berisiko tinggi bahkan menunjukkan bahwa tingkat pengetahuan seseorang tentang AI turut memoderasi kerentanan terhadap automation bias, sehingga persoalan ini tidak dapat diselesaikan hanya dengan menambah pengetahuan teknis [37].

3.2. Strategi Mengurangi False Sense of Security

Paradigma yang dominan dalam praktik keamanan organisasi adalah Information Security Awareness (ISA), yakni program yang bertujuan meningkatkan pengetahuan pengguna tentang ancaman dan prosedur aman. Premis dasarnya bersandar pada model knowledge-attitude-behavior, yaitu pengetahuan yang benar akan menghasilkan sikap yang tepat dan pada gilirannya mendorong perilaku aman. Sekti [13] pada tinjauannya yang lebih baru mengakui pentingnya ISA sekaligus menunjukkan batas-batasnya. Persoalan intinya lebih terletak pada kalibrasi kepercayaan diri yang tidak akurat daripada pada kurangnya pengetahuan. Seseorang dapat memiliki pengetahuan memadai tentang ancaman phishing namun tetap overconfident terhadap kemampuannya mendeteksi serangan, dan overconfidence itulah yang menjadi celah.

Wawasan dari teori dual-process Kahneman [14] membuka arah desain intervensi yang lebih produktif. Sistem 1 yang bekerja cepat, otomatis, dan berbasis heuristik adalah jalur pemrosesan yang dieksploitasi oleh mayoritas serangan rekayasa sosial. Sistem 2 yang bekerja lambat, deliberatif, dan analitis adalah jalur yang perlu diaktifkan agar pengguna dapat mengevaluasi situasi dengan akurat. Murayama et al. [5] menerjemahkan wawasan tersebut ke dalam konsep security friction, yaitu elemen antarmuka yang sengaja dirancang menciptakan hambatan kecil agar respons otomatis terhenti dan pengguna dipaksa berpikir sejenak tanpa mengorbankan pengalaman pengguna. Dalam operasional SOC, prinsip yang sama dapat diterapkan sebagai prosedur konfirmasi berlapis sebelum analis menutup atau mengesampingkan suatu alert.

Rahman [15] mengangkat dimensi yang kerap diabaikan dalam diskusi intervensi keamanan siber, yaitu dampak psikologis dan emosional dari insiden itu sendiri. Insiden siber menimbulkan kerugian teknis dan finansial, dan kerap pula meninggalkan kecemasan residual, learned helplessness, atau justru denial yang apabila tidak ditangani berpotensi memperburuk

ilusi keamanan di masa mendatang. Integrasi elemen ketangguhan psikologis seperti regulasi emosi, inokulasi stres, dan reframing atribusi ke dalam program pelatihan keamanan dengan demikian menjadi semakin relevan, terutama bagi analis SOC yang bekerja di bawah tekanan operasional tinggi secara berkepanjangan.

Klaim bahwa suatu intervensi efektif perlu diuji terhadap bukti empiris, bukan sekadar diasumsikan dari kelogisan mekanismenya. Ketika temuan lintas studi dibandingkan, terlihat bahwa efektivitas berbagai pendekatan sangat bervariasi bergantung pada indikator yang diukur. Pelatihan kesadaran keamanan secara konsisten meningkatkan pengetahuan dan sikap, tetapi dampaknya terhadap perubahan perilaku aktual jauh lebih kecil dan cenderung menurun seiring waktu [34], [35], [36]. Meta-analisis mengenai kepatuhan kebijakan keamanan memperkuat pola ini dengan menunjukkan bahwa faktor iklim dan norma organisasi lebih kuat memprediksi perilaku dibanding pengetahuan individual [44], [45]. Tabel 3 merangkum perbandingan bukti empiris tersebut agar arah dan kekuatan efek tiap pendekatan dapat dinilai secara setara.

Tabel 3. Perbandingan Efektivitas Empiris Strategi Intervensi terhadap False Sense of Security

Pendekatan	Bukti Empiris Utama	Arah dan Kekuatan Efek	Rujukan
Pelatihan kesadaran didaktik	Meningkatkan pengetahuan dan sikap, namun perubahan perilaku kecil dan mudah meluruh.	Positif pada kognisi, lemah pada perilaku.	[34], [35], [52]
Simulasi phishing dan latihan berbasis pengalaman	Menurunkan tingkat kegagalan pada jangka pendek, terutama saat umpan balik diberikan pada saat kesalahan terjadi.	Positif jangka pendek, meluruh tanpa penguatan.	[34], [36]
Iklim dan norma keamanan dari kepemimpinan	Iklim keamanan dan norma organisasi memprediksi kepatuhan lebih kuat daripada pengetahuan individual.	Positif, konsisten, berjangka panjang.	[44], [45]
Kolaborasi manusia dan AI pada triase alert	Penyesuaian otonomi agen menurunkan beban dan kelelahan analis; efektivitas bergantung pada desain antarmuka dan tata kelola.	Positif bersyarat pada desain.	[31], [32], [33]
Integrasi ketangguhan psikologis	Mengurangi kelelahan dan burnout analis, tetapi belum memiliki instrumen evaluasi baku.	Menjanjikan, bukti masih terbatas.	[41], [42], [43]

Tabel 3 memperjelas bahwa tidak ada pendekatan tunggal yang unggul pada semua indikator sekaligus. Pelatihan didaktik kuat memindahkan pengetahuan tetapi lemah mengubah perilaku, simulasi berbasis pengalaman efektif pada jangka pendek namun rentan meluruh tanpa penguatan, sedangkan intervensi pada tingkat iklim dan norma justru paling stabil pengaruhnya meski paling lambat terlihat. Kolaborasi manusia dan AI pada triase alert memperlihatkan hasil menjanjikan dalam menurunkan beban kognitif analis, dengan catatan bahwa efektivitasnya sangat bergantung pada desain antarmuka dan batasan wewenang yang jelas bagi otomatisasi [31], [32], [33]. Dimensi yang paling jarang tersentuh adalah kesehatan psikologis analis, padahal kelelahan kronis dan burnout terbukti melemahkan kewaspadaan dan memperbesar peluang kesalahan pada operasional SOC [41], [42], [43]. Implikasinya, intervensi yang efektif menghadapi ilusi keamanan cenderung berbentuk kombinasi beberapa pendekatan yang menargetkan kognisi individual, budaya organisasi, desain sistem, dan kesejahteraan analis secara serentak.

3.3. Cyber Resilience sebagai Kerangka Sistemik

Ketahanan siber (cyber resilience) hadir sebagai paradigma yang lebih realistis dibanding pendekatan keamanan siber konvensional. Pendekatan konvensional berfokus pada pencegahan dengan asumsi serangan dapat dihindari, sementara ketahanan siber bertolak dari pengakuan bahwa tidak semua serangan dapat dicegah. Kapasitas untuk menyerap,

merespons, dan belajar dari gangguan karenanya menjadi sama pentingnya dengan kapasitas untuk menangkalnya. NIST SP 800-160 Vol. 2 [20] mendefinisikan ketahanan siber sebagai kemampuan untuk mengantisipasi, menahan, memulihkan diri dari, dan beradaptasi terhadap kondisi yang merugikan pada sistem siber, yakni definisi yang secara eksplisit menekankan sifat dinamis.

Cano [21] mendorong kerangka tersebut lebih jauh dengan meminjam konsep antifragilitas dari Taleb [22]. Di luar sekadar tangguh yang berarti bertahan dari tekanan sambil tetap sama, sistem antifragil justru menguat karena menghadapi tekanan. Antifragilitas mensyaratkan orientasi yang secara aktif mempertanyakan asumsi keamanan yang berlaku, mencari blind spot, dan memanfaatkan setiap insiden sebagai bahan pembelajaran. Orientasi ini berseberangan secara diametral dengan iklim kognitif yang ditimbulkan oleh ilusi keamanan, ketika asumsi bahwa semuanya sudah baik justru menghalangi pengujian kritis terhadap kondisi aktual.

Singh dan Cheema [11] menyumbangkan model yang secara eksplisit menjembatani dimensi individual dan organisasional. Pada kerangka mereka tentang dimensi manusiawi ketahanan digital, bias pengambilan keputusan termasuk yang mendasari ilusi keamanan diidentifikasi sebagai penghambat langsung kapasitas resiliensi organisasi. Ketangguhan psikologis individual dinyatakan sebagai kondisi yang perlu tetapi tidak cukup. Tanpa arsitektur organisasional yang mendukung, mencakup proses yang mengkodifikasi skeptisisme, budaya yang menghargai pengakuan kegagalan, dan struktur yang memungkinkan eskalasi kekhawatiran, individu yang paling tangguh pun tidak akan dapat menghasilkan ketahanan di tingkat sistem.

Kerangka ketahanan siber yang lebih mutakhir berupaya menerjemahkan gagasan tersebut menjadi kapabilitas yang terukur. Tinjauan sistematis atas kerangka penilaian ketahanan memperlihatkan pergeseran perhatian dari pertahanan teknis menuju kesiapan organisasi yang lebih luas, mencakup deteksi, respons, dan pemulihan [49], sementara sejumlah usulan terbaru berupaya mengkuantifikasi ketahanan melalui metrik ketersediaan dan waktu pemulihan [50]. Pada tingkat operasional, kualitas kesadaran situasional analis menjadi penopang penting kapasitas ini, sebab kemampuan memahami dan memproyeksikan kondisi sistem secara akurat merupakan prasyarat respons yang tepat ketika tekanan memuncak [48]. Kesadaran situasional itu justru paling rentan tergerus ketika analis mengalami kelelahan berkepanjangan dan kekurangan dukungan, kondisi yang terdokumentasi luas sebagai persoalan modal manusia pada SOC [30]. Faktor kepercayaan dan budaya turut menentukan, karena persepsi terhadap keandalan sistem otomatis membentuk kesediaan analis untuk memvalidasi ulang keluarannya [51], sedangkan budaya keamanan yang matang menautkan kewaspadaan individual dengan proses organisasi yang menghargai pengakuan kesalahan [53].

3.4. Temuan pada Akar Psikologis

Hasil sintesis literatur memperlihatkan bahwa ilusi keamanan terbentuk dari interaksi beberapa faktor psikologis yang saling memperkuat. Sintesis atas berbagai studi mengenai faktor manusia pada keamanan organisasi menunjukkan tiga anteseden yang konsisten muncul sebagai pendahulu kegagalan keamanan, yaitu overconfidence, kerentanan terhadap rekayasa sosial, dan normalisasi perilaku menyimpang. Temuan yang paling menonjol adalah bahwa persepsi keamanan, dan bukan kondisi teknis aktual, menjadi prediktor terkuat apakah pengguna akan mengambil tindakan pengamanan tambahan. Artinya, seseorang yang merasa aman cenderung tidak melakukan langkah ekstra, terlepas dari apakah rasa amannya beralasan atau tidak.

Sejumlah studi kualitatif pada beberapa organisasi mengungkap pola yang serupa. Pengguna yang memodifikasi atau mengabaikan kebijakan keamanan umumnya bertindak demikian karena yakin solusi alternatif yang mereka rancang sendiri sudah cukup aman, bukan karena malas atau tidak peduli. Keyakinan tersebut keliru, namun nyata dan kuat, sehingga sulit diluruhkan hanya dengan penambahan informasi teknis. Pola yang sama juga teramati pada tingkat organisasi, ketika kebiasaan pengambilan keputusan kolektif dan budaya internal terbukti rentan mengalami degradasi serupa.

Penelitian mengenai SOC dan Security Information and Event Management (SIEM) menambahkan dimensi operasional yang penting bagi pembahasan ini. Analis yang terlalu mengandalkan automated threat detection cenderung mengurangi proses validasi manual dan menurunkan kewaspadaan terhadap anomali yang memerlukan penilaian kontekstual, yakni jenis ancaman yang justru paling mungkin lolos dari filter otomatis. Pada level organisasi,

fenomena yang dikenal sebagai compliance theater juga teramati cukup luas, yaitu kondisi ketika dokumentasi kebijakan keamanan dipelihara dengan sangat lengkap tetapi tidak diiringi praktik operasional yang setara. Kondisi tersebut dapat dipandang sebagai analog institusional dari ilusi keamanan individual.

3.5. Temuan pada Efektivitas Strategi Intervensi

Hasil sintesis pada dimensi intervensi memperlihatkan bahwa iklim keamanan, yakni seberapa nyata kepedulian terhadap keamanan tercermin pada perilaku kepemimpinan sehari-hari, jauh lebih kuat memprediksi kepatuhan kebijakan dibanding pengetahuan individual karyawan. Implikasinya bagi pengelolaan SOC cukup tegas. Investasi pada pelatihan teknis tanpa disertai perubahan sinyal budaya dari kepemimpinan kemungkinan besar tidak akan mengubah perilaku secara berkelanjutan, sebab perilaku organisasional pada umumnya merespons isyarat dari atas lebih dulu sebelum merespons konten pelatihan.

Temuan menonjol berikutnya adalah fenomena habituasi yang berkaitan langsung dengan alert fatigue di SOC. Pada berbagai studi lapangan, pengguna yang terpapar terlalu sering pada peringatan keamanan belajar mengabaikan peringatan tersebut secara refleks. Sistem yang dirancang untuk meningkatkan kewaspadaan dengan demikian justru secara sistematis melatih penggunanya untuk mengabaikan sinyal bahaya. Tingkat gangguan visual, biaya interaksi, dan kejelasan penjelasan konsekuensi merupakan faktor desain yang paling signifikan memoderasi laju habituasi tersebut, sehingga ketiganya layak menjadi titik fokus dalam perancangan ulang antarmuka peringatan.

Pendekatan berbasis pengalaman langsung memperlihatkan hasil yang lebih menjanjikan dibanding pendekatan didaktik. Simulasi serangan siber yang realistis, yaitu ketika peserta mengalami sendiri konsekuensi keputusan keamanan yang buruk pada lingkungan aman, terbukti lebih efektif menurunkan overconfidence dibanding pelatihan konvensional. Pengalaman langsung memberikan umpan balik yang mengkalibrasi ulang keyakinan dengan cara yang sulit dicapai melalui modul e-learning. Pendekatan tersebut sangat relevan untuk latihan red team dan tabletop exercise pada SOC.

Tabel 4. Perbandingan Pendekatan Intervensi terhadap False Sense of Security

Pendekatan	Mekanisme Kerja	Keterbatasan
ISA tradisional	Memberikan pengetahuan ancaman dan prosedur aman melalui pelatihan didaktik.	Tidak menyentuh kalibrasi kepercayaan diri sehingga overconfidence tetap bertahan.
Security friction	Menyisipkan hambatan kecil pada antarmuka untuk memicu pemrosesan deliberatif.	Efektivitas tergantung pada desain dan dapat menimbulkan gesekan berlebih jika tidak dikalibrasi.
Simulasi dan gamifikasi	Memberikan pengalaman langsung konsekuensi keputusan buruk pada lingkungan aman.	Memerlukan sumber daya skenario yang relevan dan terus diperbarui.
Iklim keamanan kepemimpinan	Mengubah sinyal budaya melalui keteladanan dan komitmen visible dari pimpinan.	Perubahan bersifat jangka panjang dan sulit diukur dalam kurun pendek.
Integrasi ketangguhan psikologis	Memasukkan regulasi emosi dan inokulasi stres ke dalam pelatihan analis.	Belum memiliki standar implementasi dan instrumen evaluasi yang baku.

Tabel 4 di atas menunjukkan bahwa tidak ada pendekatan tunggal yang dapat dianggap sebagai jalan keluar penuh. Setiap pendekatan menargetkan mekanisme yang berbeda, mulai dari kognisi individual hingga budaya kepemimpinan. Implikasinya, intervensi yang efektif

kemungkinan besar berbentuk kombinasi dari beberapa pendekatan tersebut yang disesuaikan dengan profil risiko dan kapasitas organisasi.

3.6. Temuan pada Peran Ketahanan Siber

Perbandingan respons sejumlah organisasi terhadap insiden siber signifikan menghasilkan temuan yang penting. Pembeda utama antara organisasi berketahanan tinggi dan organisasi yang lemah ketahanannya lebih ditentukan oleh kualitas proses manusiawi dalam merespons daripada oleh kecanggihan teknologi pertahanan. Aspek tersebut mencakup kejelasan komunikasi kepemimpinan saat krisis, koordinasi lintas fungsi yang cepat, dan kemampuan mempertahankan kesadaran situasional yang akurat ketika tekanan paling tinggi. Organisasi yang sebelumnya memperlihatkan tanda-tanda ilusi keamanan, seperti kepuasan berlebih terhadap postur pertahanan yang ada, konsisten menunjukkan waktu respons lebih lambat dan biaya pemulihan lebih besar.

Pengembangan model kematangan budaya keamanan informasi memberikan perspektif lain yang melengkapi. Organisasi pada tingkat kematangan tinggi, yakni ketika norma keamanan sudah terinternalisasi sebagai bagian dari identitas dan kebiasaan sehari-hari dan bukan sekadar daftar prosedur yang dijalankan karena kewajiban kepatuhan, memperlihatkan kemampuan deteksi dan respons ancaman yang signifikan lebih baik. Kematangan semacam ini tidak dapat dipasang secara instan, melainkan tumbuh dari kepemimpinan yang konsisten, sistem umpan balik yang jujur, dan kesediaan institusional untuk mengakui bahwa persepsi keamanan yang dimiliki mungkin salah.

Analisis pasca-insiden terhadap sejumlah kasus ransomware pada organisasi besar memberikan bukti paling konkret tentang ilusi keamanan di tingkat institusional. Pada hampir semua kasus yang diteliti, asesmen keamanan internal sebelum insiden menyatakan bahwa organisasi sudah terlindungi dengan memadai. Kesenjangan antara penilaian diri tersebut dengan kerentanan aktual yang kemudian terbukti mengisyaratkan bahwa metodologi asesmen keamanan yang umum digunakan secara struktural dapat menghasilkan false assurance, terutama ketika asesmen dilakukan secara internal tanpa mekanisme tantangan independen. Pada lingkungan cloud dan operasi berbasis AI, ketergantungan pada automated compliance reporting menimbulkan risiko struktural yang serupa.

3.7. Rangkuman Celah Riset

Sintesis lintas tiga dimensi tersebut menghasilkan gambaran yang koheren. Ilusi keamanan berfungsi sebagai variabel penghubung yang mengikat kerentanan psikologis individual, efektivitas desain intervensi, dan kapasitas ketahanan siber pada tingkat organisasi. Beberapa celah riset paling menonjol diringkas pada Tabel 5 berikut.

Tabel 5. Rangkuman Celah Riset Lintas Dimensi

Dimensi	Celah Riset yang Teridentifikasi
Akar psikologis	Validitas eksternal temuan untuk konteks UMKM, sektor publik negara berkembang, dan pengguna non-korporat masih terbatas. Dampak adopsi AI dan automation terhadap tingkat ilusi keamanan analis SOC juga belum mendapat perhatian empiris memadai.
Strategi intervensi	Mayoritas studi masih bergantung pada self-report dan tugas laboratorium. Data efektivitas jangka panjang melampaui enam bulan nyaris tidak tersedia, dan intervensi khusus untuk blind trust terhadap automation belum dirancang secara sistematis.
Ketahanan siber	Operasionalisasi ketahanan siber masih heterogen lintas framework. Perhatian penelitian terkonsentrasi pada organisasi besar sehingga UMKM kurang terlayani. Studi prospektif yang menguji hubungan kausal antara ilusi keamanan pra-insiden dan hasil ketahanan organisasional belum tersedia.

Tabel 5 memperjelas bahwa kebutuhan riset tidak terbatas pada satu dimensi tertentu, tetapi tersebar pada ketiga lapis fenomena. Pada dimensi akar psikologis, persoalan utama

adalah konteks dan modernisasi alat. Pada dimensi intervensi, persoalan utama adalah metodologi dan ketahanan dampak. Pada dimensi ketahanan siber, persoalan utama adalah generalisabilitas dan inferensi kausal.

3.8. Keterbatasan Kajian

Kajian ini memiliki sejumlah keterbatasan yang perlu dipertimbangkan dalam menafsirkan temuannya. Cakupan basis data, meskipun mencakup lima sumber utama, berpotensi melewatkan literatur yang terbit pada kanal regional atau berbahasa selain Inggris dan Indonesia, sehingga sebagian perspektif dari konteks negara berkembang mungkin kurang terwakili. Pembatasan bahasa dan ketersediaan teks penuh juga menyempitkan populasi artikel yang dapat ditelaah secara mendalam. Selain itu, sebagai tinjauan literatur, kajian ini bertumpu pada temuan yang telah dipublikasikan sehingga rentan terhadap bias publikasi, ketika studi dengan hasil signifikan lebih mungkin terbit dibanding studi dengan hasil nol.

Keterbatasan berikutnya berkaitan dengan sifat sintesis yang dilakukan. Heterogenitas desain, konteks, dan indikator antar studi membuat perbandingan efektivitas intervensi bersifat kualitatif dan tidak memungkinkan penggabungan ukuran efek secara kuantitatif. Sebagian bukti mengenai konteks SOC dan otomatisasi berbasis AI juga masih terbatas dan bertumpu pada studi berskala kecil atau simulasi laboratorium, sehingga generalisasinya perlu diuji lebih lanjut. Interpretasi tematik, meskipun telah melalui pemeriksaan silang antarpenulis, tetap mengandung unsur penilaian subjektif. Keterbatasan-keterbatasan tersebut sekaligus menegaskan perlunya penelitian empiris lanjutan, khususnya pengembangan dan pengujian instrumen pengukuran ilusi keamanan pada lingkungan operasional SOC.

4. Kesimpulan

Kajian ini menegaskan bahwa false sense of security merupakan persoalan penting dalam operasional SOC modern karena rasa aman dapat terbentuk bahkan ketika risiko sebenarnya belum sepenuhnya terkendali. Dalam lingkungan yang banyak bergantung pada SIEM, SOAR, threat intelligence platform, dan AI-driven monitoring, analis dapat terdorong untuk mempercayai dashboard, status alert, atau rekomendasi sistem secara berlebihan. Kondisi ini membuat proses validasi manual menjadi semakin penting, terutama ketika ancaman tidak muncul sebagai alert kritis atau berjalan melalui pola yang tidak mudah dikenali oleh sistem otomatis.

Hasil sintesis menunjukkan bahwa false sense of security dipengaruhi oleh kombinasi faktor psikologis, teknis, dan organisasional. Bias kognitif, cybercomplacency, automation bias, alert fatigue, serta budaya organisasi yang terlalu berorientasi pada kepatuhan dapat saling memperkuat dan melemahkan kewaspadaan analis. Dengan kata lain, keamanan tidak cukup dinilai dari lengkapnya kontrol, rendahnya jumlah alert, atau terpenuhinya laporan kepatuhan. Organisasi perlu memastikan bahwa setiap indikator keamanan tetap diuji melalui pembacaan konteks, validasi lintas sumber data, dan proses eskalasi yang jelas.

Intervensi untuk mengurangi ilusi keamanan tidak dapat hanya mengandalkan pelatihan kesadaran keamanan yang bersifat umum. SOC membutuhkan pendekatan yang lebih dekat dengan praktik kerja analis, seperti simulasi insiden, tabletop exercise, red team exercise, evaluasi false positive, penguatan budaya validasi, serta desain otomatisasi yang tetap memberi ruang bagi penilaian manusia. AI dan otomatisasi perlu diposisikan sebagai alat bantu pengambilan keputusan, bukan sebagai pengganti kewaspadaan analis.

Dari perspektif cyber resilience, organisasi yang tangguh adalah organisasi yang mampu mengenali keterbatasan sistemnya sendiri, bukan sekadar yang memiliki teknologi keamanan lengkap. Ketahanan siber menuntut kemampuan untuk mendeteksi lebih cepat, merespons lebih tepat, memulihkan layanan, dan belajar dari setiap insiden. Oleh karena itu, pengurangan false sense of security perlu menjadi bagian dari strategi peningkatan cyber resilience, terutama pada SOC yang semakin bergantung pada otomatisasi dan kecerdasan buatan.

Penelitian selanjutnya disarankan untuk mengembangkan instrumen pengukuran false sense of security yang sesuai dengan konteks operasional SOC. Instrumen tersebut perlu mengukur pengetahuan keamanan sekaligus tingkat kepercayaan terhadap sistem otomatis, kecenderungan mengabaikan validasi manual, persepsi terhadap alert, dan budaya eskalasi dalam organisasi. Selain itu, penelitian empiris diperlukan untuk menguji apakah penurunan false sense of security pada analis SOC berhubungan dengan peningkatan indikator cyber resilience, seperti kecepatan deteksi, ketepatan respons, dan efektivitas pemulihan insiden.

Daftar Pustaka

[1] T. F. Stafford, "Cybercomplacency: Cognitive complacency in the security domain," Journal of Computer Information Systems, vol. 57, no. 1, pp. 1-8, 2017.

[2] J. R. C. Nurse, "Cybersecurity challenges in the age of AI, automation, and digital transformation," IEEE Security & Privacy, vol. 19, no. 3, pp. 4-7, 2021.

[3] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," Econometrica, vol. 47, no. 2, pp. 263-291, 1979.

[4] R. West, "The psychology of security," Communications of the ACM, vol. 51, no. 4, pp. 34-40, 2008.

[5] Y. Murayama, M. Fujii, and D. Nishioka, "Sense of security and warning interface design in cyberspace," International Journal of Human-Computer Studies, vol. 69, no. 10, pp. 658-667, 2011.

[6] T. F. Stafford, "Cybercomplacency and behavioral cybersecurity risk," Journal of Computer Information Systems, vol. 57, no. 1, pp. 1-8, 2017.

[7] B. Khan, S. B. Maynard, and A. Ahmad, "A systematic review of cyber resilience frameworks," Computers & Security, vol. 120, p. 102800, 2022.

[8] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," Journal of Psychology, vol. 91, no. 1, pp. 93-114, 1975.

[9] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "The human aspects of information security questionnaire (HAIS-Q): Two further validation studies," Computers & Security, vol. 66, pp. 40-51, 2017.

[10] A. Adams and M. A. Sasse, "Users are not the enemy," Communications of the ACM, vol. 42, no. 12, pp. 40-46, 1999.

[11] R. Singh and A. Cheema, "Human dimensions of digital resilience: Cognitive biases, decision-making, and cyber defense," International Journal of Digital Resilience, vol. 3, no. 2, pp. 45-62, 2024.

[12] R. Montesino and S. Fenz, "Information security automation: How far can we go?" in Proc. 6th Int. Conf. Availability, Reliability and Security (ARES), Vienna, Austria, 2011, pp. 280-285.

[13] B. W. Sekti, "Information security awareness and the mitigation of cybersecurity complacency in organizational settings," Journal of Information Security and Applications, vol. 79, p. 103621, 2025.

[14] D. Kahneman, Thinking, Fast and Slow. New York, NY, USA: Farrar, Straus and Giroux, 2011.

[15] N. A. A. Rahman, "Psychological resilience and cybersecurity: Integrating mental health frameworks into organizational security policies," Cybersecurity Journal, vol. 8, no. 1, pp. 12-28, 2025.

[16] W. Rocha Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," Computers & Security, vol. 59, pp. 26-44, 2016.

[17] S. Egelman and A. P. Felt, "Malefactor-resistant user interfaces," in Proc. Workshop on Home Usable Privacy and Security (HUPS), Washington, DC, USA, 2012.

[18] D. Akhawe and A. P. Felt, "Alice in Warningland: A large-scale field study of browser security warning effectiveness," in Proc. 22nd USENIX Security Symposium, Washington, DC, USA, 2013, pp. 257-272.

[19] S. Scholefield and L. A. Shepherd, "Gamification techniques for raising cyber security awareness," in Proc. 18th European Conference on Cyber Warfare and Security, Coimbra, Portugal, 2019, pp. 466-475.

[20] National Institute of Standards and Technology, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST SP 800-160 Vol. 2. Gaithersburg, MD, USA: U.S. Dept. of Commerce, 2021.

[21] J. Cano, "Cyber resilience and antifragility: Navigating volatility, uncertainty, complexity, and ambiguity in digital environments," Journal of Cybersecurity and Privacy, vol. 1, no. 3, pp. 462-476, 2021.

[22] N. N. Taleb, Antifragile: Things That Gain from Disorder. New York, NY, USA: Random House, 2012.

[23] F. Bjorck, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber resilience: Fundamentals for a definition," in Proc. 4th Int. Conf. New Contributions in Information Systems and Technologies, 2015, pp. 311-316.

[24] A. Da Veiga, L. V. Astakhova, A. Botha, and M. Herselman, "Defining organisational information security culture: Perspectives from academia and industry," Computers & Security, vol. 92, p. 101713, 2020.

[25] L. Y. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures," Computers & Security, vol. 87, p. 101568, 2019.

[26] M. E. Whitman and H. J. Mattord, Principles of Information Security, 6th ed. Boston, MA, USA: Cengage Learning, 2021.

[27] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Computers & Security, vol. 98, p. 102003, 2020.

[28] B. A. Alahmadi, L. Axon, and I. Martinovic, "99% false positives: A qualitative study of SOC analysts' perspectives on security alarms," in Proc. 31st USENIX Security Symposium, Boston, MA, USA, 2022, pp. 2783-2800.

[29] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupe, and G.-J. Ahn, "Matched and mismatched SOCs: A qualitative study on security operations center issues," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), London, UK, 2019, pp. 1955-1970.

[30] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in Proc. 11th Symp. Usable Privacy and Security (SOUPS), Ottawa, ON, Canada, 2015, pp. 347-359.

[31] M. Baruwal Chhetri, S. Tariq, R. Singh, F. Jalalvand, C. Paris, and S. Nepal, "Towards human-AI teaming to mitigate alert fatigue in security operations centres," ACM Trans. Internet Technol., vol. 24, no. 3, pp. 1-22, 2024.

[32] D. Schlette, P. Empl, M. Caselli, T. Schreck, and G. Pernul, "Do you play it by the books? A study on incident response playbooks and influencing factors," in Proc. IEEE Symp. Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 3625-3643.

[33] R. Singh, S. Tariq, F. Jalalvand, M. Baruwal Chhetri, S. Nepal, C. Paris, and M. Lochner, "LLMs in the SOC: An empirical study of human-AI collaboration in security operations centres," arXiv preprint arXiv:2508.18947, 2025.

[34] D. Hillman, Y. Harel, and E. Toch, "Evaluating organizational phishing awareness training on an enterprise scale," Computers & Security, vol. 132, p. 103364, 2023.

[35] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior," IEEE Access, vol. 10, pp. 132132-132143, 2022.

[36] D. Sikolia, D. Biros, and T. Zhang, "How effective are SETA programs anyway: Learning and forgetting in security awareness training," Journal of Cybersecurity Education, Research and Practice, vol. 2023, no. 1, 2023.

[37] M. C. Horowitz and L. Kahn, "Bending the automation bias curve: A study of human and AI-based decision making in national security contexts," International Studies Quarterly, vol. 68, no. 2, sqae020, 2024.

[38] R. Parasuraman and D. H. Manzey, "Complacency and bias in human use of automation: An attentional integration," Human Factors, vol. 52, no. 3, pp. 381-410, 2010.

[39] L. J. Skitka, K. L. Mosier, and M. Burdick, "Does automation bias decision-making?" International Journal of Human-Computer Studies, vol. 51, no. 5, pp. 991-1006, 1999.

[40] J. D. Lee and K. A. See, "Trust in automation: Designing for appropriate reliance," Human Factors, vol. 46, no. 1, pp. 50-80, 2004.

[41] C. Nobles, "Stress, burnout, and security fatigue in cybersecurity: A human factors problem," HOLISTICA - Journal of Business and Public Administration, vol. 13, no. 1, pp. 49-72, 2022.

[42] T. Singh, A. C. Johnston, J. D'Arcy, and P. D. Harms, "Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research," Organizational Cybersecurity Journal: Practice, Process and People, vol. 3, no. 2, pp. 100-126, 2023.

[43] A. Reeves, M. Pattinson, and M. Butavicius, "Is your CISO burnt out yet? Examining demographic differences in workplace burnout amongst cyber security professionals," in Human Aspects of Information Security and Assurance (HAISA). Cham, Switzerland: Springer, 2023, pp. 225-236.

[44] W. A. Cram, J. D'Arcy, and J. G. Proudfoot, "Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance," MIS Quarterly, vol. 43, no. 2, pp. 525-554, 2019.

[45] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance," MIS Quarterly, vol. 42, no. 1, pp. 285-311, 2018.

[46] N. D. Weinstein, "Unrealistic optimism about future life events," Journal of Personality and Social Psychology, vol. 39, no. 5, pp. 806-820, 1980.

[47] A. Tversky and D. Kahneman, "Judgment under uncertainty: Heuristics and biases," Science, vol. 185, no. 4157, pp. 1124-1131, 1974.

[48] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," Human Factors, vol. 37, no. 1, pp. 32-64, 1995.

[49] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience," Sensors, vol. 23, no. 16, p. 7273, 2023.

[50] S. M. AlHidaifi, M. R. Asghar, and I. S. Ansari, "Towards a cyber resilience quantification framework (CRQF) for IT infrastructure," Computer Networks, vol. 247, p. 110446, 2024.

[51] T. Araujo, N. Helberger, S. Kruikemeier, and C. H. de Vreese, "In AI we trust? Perceptions about automated decision-making by artificial intelligence," AI & Society, vol. 35, no. 3, pp. 611-623, 2020.

[52] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?" in Proc. Int. Conf. Cyber Security for Sustainable Society, Coventry, UK, 2019, pp. 118-131.

[53] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," Computers & Security, vol. 29, no. 2, pp. 196-207, 2010.