Arus Jurnal Sosial dan Humaniora (AJSH)
Website: http://jurnal.ardenjaya.com/index.php/ajsh
Email: jurnal.ajsh@ardenjaya.com

Dampak Pendekatan Cyber Security terhadap Pengamanan Operasi Industri Minyak dan Gas (Migas) di Indonesia

INFO PENULIS

Gunawan Hidayat
Universitas Muhammadiyah Jakarta
gunawan.hidayat@umj.ac.id

Iswadi
Universitas Esa Unggul
iswadi@esaunggul.ac.id

INFO ARTIKEL

ISSN: 2808-1307
Vol. 5, No. 3, Desember 2025
https://jurnal.ardenjaya.com/index.php/ajsh

© 2025 Arden Jaya Publisher All rights reserved

Saran Penulisan Referensi:

Hidayat, G., & Iswadi. (2025). Dampak Pendekatan Cyber Securiry terhadap Pengamanan Operasi Industri Minyak dan Gas (Migas) di Indonesia. *Arus Jurnal Sosial dan Humaniora, 5* (3), 5141-5150.

Abstrak

Penelitian ini bertujuan untuk menganalisis profil ancaman siber yang dihadapi industri minyak dan gas (migas) di Indonesia, menelaah pendekatan cyber security yang telah diterapkan, menilai dampaknya terhadap pengamanan operasi industri, serta menelusuri berbagai kendala dan faktor penghambat yang dihadapi perusahaan migas dalam mengimplementasikan strategi cyber security. Metode penelitian menggunakan pendekatan mixed methods, yang memadukan analisis kuantitatif untuk mengukur pengaruh penerapan cyber security terhadap tingkat pengamanan operasi, dan analisis kualitatif untuk memperdalam pemahaman mengenai kendala serta strategi implementasi di lapangan. Teknik pengumpulan data dilakukan melalui penyebaran kuesioner kepada tenaga ahli dan praktisi IT/OT security, wawancara mendalam dengan regulator dan pakar industri migas, serta dokumentasi berupa laporan perusahaan, regulasi pemerintah, dan laporan industri terkait keamanan siber. Hasil penelitian menunjukkan bahwa ancaman utama yang dihadapi meliputi serangan ransomware, phishing, supply chain attack, hingga gangguan pada sistem kontrol industri (ICS/SCADA). Pendekatan cyber security yang diterapkan, seperti segmentasi jaringan IT–OT, intrusion detection system, manajemen patch, pelatihan kesadaran, dan threat intelligence, terbukti meningkatkan ketahanan sistem operasi dengan menekan frekuensi insiden dan mempercepat pemulihan. Namun, implementasi masih menghadapi hambatan berupa keterbatasan SDM, tingginya biaya investasi teknologi, dan koordinasi regulasi yang belum optimal.

Kata Kunci: Cyber Security, Industri Migas, Indonesia, Pengamanan Operasi, Infrastruktur Kritis

Abstract

This study aims to analyze the cyber threat profile faced by the oil and gas industry in Indonesia, examine the cyber security approaches that have been implemented, assess their impact on securing industrial operations, and identify various constraints and inhibiting factors encountered by oil and gas companies in implementing cyber security strategies. The research employs a mixed-methods approach, combining quantitative analysis to measure the effect of cyber security implementation on the level of operational security, and qualitative analysis to deepen the understanding of implementation challenges and strategies in practice. Data collection techniques include the distribution of questionnaires to IT/OT security experts and practitioners, in-depth interviews with regulators and oil and gas industry experts, and documentation in the form of company reports, government regulations, and industry reports related to cyber security. The results indicate that the main threats include ransomware attacks, phishing, supply chain attacks, and disruptions to industrial control systems (ICS/SCADA). Cyber security approaches such as IT–OT network segmentation, intrusion detection systems, patch management, security awareness training, and threat intelligence have been shown to enhance operational system resilience by reducing incident frequency and accelerating recovery. However, implementation still faces obstacles in the form of limited human resources, high technology investment costs, and suboptimal regulatory coordination.

Keywords: Cyber Security, Oil and Gas Industry, Indonesia, Operational Security, Critical Infrastructure

A. Pendahuluan

Industri minyak dan gas (migas) merupakan salah satu infrastruktur kritikal yang memegang peranan strategis dalam ketahanan energi dan pembangunan ekonomi nasional Indonesia. Sektor ini bukan hanya menyumbang penerimaan negara, tetapi juga menjadi penopang utama dalam menjaga ketersediaan energi domestik. Transformasi digital yang semakin pesat mendorong perusahaan migas untuk mengadopsi sistem kendali industri (Industrial Control Systems/ICS), Supervisory Control and Data Acquisition (SCADA), serta integrasi teknologi informasi (IT) dan teknologi operasional (OT). Inovasi ini memungkinkan efisiensi produksi, optimasi rantai pasok, hingga pemantauan kondisi aset secara real-time (KPMG, 2024). Namun, di balik manfaat tersebut, keterhubungan sistem IT dan OT menimbulkan kerentanan baru terhadap ancaman siber.

Ancaman siber terhadap sektor energi, termasuk migas, semakin kompleks dan canggih. Laporan *Dragos OT Cybersecurity Year in Review* (2025) menunjukkan peningkatan signifikan dalam jumlah serangan siber yang menargetkan ICS/OT, termasuk serangan ransomware yang dapat menghentikan operasi kilang atau jaringan distribusi energi secara total. Ancaman ini bukan hanya berdampak pada kerugian finansial, melainkan juga pada keselamatan pekerja, keamanan lingkungan, serta keberlangsungan pasokan energi nasional. Faktor yang memperbesar risiko antara lain usia infrastruktur yang relatif tua, keterbatasan patch keamanan, keterlibatan vendor pihak ketiga, serta keterbatasan visibilitas jaringan OT (Dragos, 2025).

Kasus serangan siber global telah membuktikan dampaknya yang nyata. Insiden ransomware terhadap Colonial Pipeline di Amerika Serikat pada 2021, misalnya, menyebabkan kelumpuhan distribusi bahan bakar di sebagian besar wilayah timur AS, menimbulkan kerugian ekonomi miliaran dolar, dan memicu kepanikan publik (Lee et al., 2022). Walaupun kasus tersebut terjadi di luar negeri, pelajaran penting dapat ditarik untuk Indonesia, karena pola serangan yang sama berpotensi menyasar infrastruktur energi domestik.

Indonesia sendiri tidak terlepas dari ancaman ini. Beberapa tahun terakhir, serangan siber terhadap lembaga pemerintah dan infrastruktur kritikal semakin marak. Pada 2024, serangan ransomware terhadap Pusat Data Nasional menyebabkan gangguan layanan publik, menegaskan bahwa infrastruktur digital negara masih rentan terhadap ancaman siber berskala besar (Reuters, 2024). Hal ini memperlihatkan urgensi peningkatan ketahanan siber, khususnya di sektor strategis seperti migas, yang memiliki keterkaitan erat dengan stabilitas ekonomi dan keamanan nasional.

Studi yang dilakukan Fortinet (2024) menemukan bahwa perusahaan migas global menghadapi tantangan ganda: di satu sisi mereka dituntut untuk melakukan digitalisasi guna

meningkatkan daya saing, namun di sisi lain investasi dalam *cyber security* OT masih relatif rendah dibandingkan sektor keuangan atau telekomunikasi. Kondisi ini juga terlihat di Indonesia, di mana adopsi teknologi baru dalam operasi migas belum sepenuhnya diimbangi dengan peningkatan keamanan yang memadai (Fortinet, 2024).

Selain faktor teknis, aspek organisasi dan kebijakan juga memegang peranan penting dalam efektivitas pendekatan *cyber security*. Keberhasilan implementasi tidak hanya bergantung pada ketersediaan perangkat keras atau perangkat lunak, tetapi juga pada tata kelola (governance), kesadaran karyawan, serta regulasi yang mendukung. Dalam konteks Indonesia, Undang-Undang Perlindungan Data Pribadi dan Peraturan Badan Siber dan Sandi Negara (BSSN) memberikan kerangka dasar, namun penerapan di level korporasi sering kali menghadapi kendala seperti keterbatasan sumber daya manusia yang memiliki kompetensi khusus di bidang OT security (BSSN, 2023).

Tantangan ini semakin relevan karena tren peningkatan eksplorasi dan produksi migas nasional. Pemerintah menargetkan peningkatan produksi minyak menjadi 1 juta barel per hari dan gas 12 BSCFD pada 2030. Ambisi ini menuntut investasi besar pada infrastruktur baru, yang pada gilirannya meningkatkan eksposur risiko siber. Setiap lokasi operasi baru berarti menambah titik potensi serangan yang harus diamankan (Pertamina, 2024). Dengan demikian, pendekatan *cyber security* yang komprehensif menjadi kebutuhan mendesak, bukan hanya pilihan.

Berbagai pendekatan *cyber security* telah diusulkan dan diterapkan dalam industri migas, mulai dari segmentasi jaringan IT dan OT, pemantauan anomali berbasis kecerdasan buatan, manajemen kerentanan secara berkala, hingga peningkatan kapabilitas deteksi dan respons insiden (Automation.com, 2024). Namun, efektivitas dari langkah-langkah tersebut masih perlu diteliti lebih jauh, khususnya dalam konteks operasional migas di Indonesia. Sebagian besar literatur masih berfokus pada studi kasus di luar negeri, sementara kondisi domestik memiliki karakteristik yang unik, baik dari sisi regulasi, sumber daya manusia, maupun kondisi infrastruktur.

Kesenjangan inilah yang ingin dijawab oleh penelitian ini. Penelitian mengenai dampak pendekatan *cyber security* terhadap pengamanan operasi industri migas di Indonesia menjadi penting untuk mengetahui sejauh mana strategi yang telah diterapkan efektif dalam memitigasi risiko, apa hambatan yang dihadapi dalam implementasi, dan indikator apa yang dapat digunakan untuk mengukur keberhasilan. Hasil penelitian diharapkan dapat memberikan kontribusi teoretis dalam pengembangan literatur mengenai *cyber security* OT, sekaligus kontribusi praktis bagi pengambil keputusan di sektor migas dan regulator nasional.

Penelitian ini memiliki kontribusi penting dalam dua dimensi utama. Pertama, dari sisi akademis, penelitian ini berkontribusi pada pengembangan literatur mengenai *cyber security* dalam konteks sektor energi, khususnya industri migas di Indonesia yang masih relatif minim kajian empiris. Penelitian ini dapat memperluas perspektif teoretis tentang hubungan antara pendekatan *cyber security* dengan keberlangsungan operasi industri berbasis OT/ICS, serta memberikan bukti empiris yang relevan untuk menutup celah penelitian yang selama ini ada.

Kedua, dari sisi praktis, penelitian ini memberikan manfaat langsung bagi para pemangku kepentingan, baik regulator, perusahaan migas, maupun penyedia solusi keamanan. Hasil penelitian dapat digunakan sebagai dasar penyusunan kebijakan strategis, peningkatan standar operasional keamanan OT, dan perancangan program pelatihan serta kesadaran siber yang lebih efektif. Pada tataran makro, hasil penelitian berpotensi mendukung terciptanya ekosistem operasi migas yang lebih aman, andal, dan berkelanjutan, sekaligus memperkuat ketahanan energi nasional di tengah meningkatnya ancaman siber yang kompleks dan dinamis. Dengan kata lain, temuan penelitian ini diharapkan mampu menjadi jembatan antara teori, praktik, dan kebijakan publik.

Berdasarkan latar belakang tersebut, penelitian ini diarahkan untuk menjawab beberapa pokok persoalan utama. Pertama, penelitian ini ingin memahami bagaimana profil dan karakteristik ancaman siber yang dihadapi oleh industri migas di Indonesia, khususnya dalam konteks keterhubungan sistem IT dan OT yang semakin kompleks. Kedua, penelitian ini berupaya menelaah berbagai pendekatan *cyber security* yang telah diterapkan dalam operasi migas serta sejauh mana implementasinya berjalan efektif di lapangan. Ketiga, penelitian ini akan mengkaji dampak nyata dari penerapan pendekatan *cyber security* terhadap tingkat pengamanan operasi, baik dari sisi teknis maupun operasional. Terakhir, penelitian ini juga akan menelusuri berbagai kendala dan faktor penghambat yang dihadapi perusahaan migas dalam mengimplementasikan strategi *cyber security*.

Dengan merumuskan pertanyaan-pertanyaan penelitian tersebut, diharapkan kajian ini dapat memberikan gambaran yang komprehensif mengenai efektivitas pendekatan *cyber security*

sekaligus menyumbang rekomendasi strategis untuk memperkuat ketahanan energi nasional melalui pengamanan operasi industri migas.

Konsep dan ruang lingkup *cyber security* pada OT/ICS

Cyber security pada lingkungan industri (Operational Technology/OT) dan Industrial Control Systems (ICS) berbeda karakter dibandingkan keamanan IT tradisional karena keterkaitan langsung dengan proses fisik—mis. pengendalian pompa, katup, atau sistem distribusi energi—yang apabila terganggu dapat menimbulkan dampak fisik dan keselamatan (KPMG, 2024). Oleh karena itu, literatur membedakan antara pengamanan IT (confidentiality, integrity, availability) dan prioritas pada OT yang sering memberi bobot tinggi pada availability dan safety. Pemahaman konseptual ini penting untuk menilai dampak kebijakan atau intervensi *cyber security* terhadap operasi migas. (KPMG, 2024).

Tren ancaman global terhadap sektor industri/energi

Beberapa laporan industri menunjukkan peningkatan tajam serangan yang menarget OT dan sektor energi. Dragos (2025) mencatat lonjakan serangan ransomware terhadap organisasi industri, serta kemunculan kelompok pelaku yang menarget sektor energi dan utilitas dengan teknik yang semakin canggih (mis. custom backdoors, supply chain compromise). Fortinet (2024) menegaskan tren intrusi yang mempengaruhi OT dan gabungan IT–OT, serta peningkatan insiden akibat phishing dan kompromi email sebagai titik awal (Fortinet, 2024; Dragos, 2025). Temuan ini mengindikasikan bahwa ancaman bukan hanya lebih sering tetapi juga lebih terfokus pada infrastruktur kritis.

Pendekatan dan praktik mitigasi yang banyak direkomendasikan

Literatur praktis dan laporan konsultan mengelompokkan pendekatan mitigasi ke beberapa domain utama: segmentasi jaringan IT–OT; manajemen patch dan kerentanan; monitoring & threat detection (termasuk solusi berbasis anomaly detection/AI); manajemen identitas dan akses (IAM) untuk akses operator dan vendor; rencana respons insiden & business continuity; serta peningkatan kapabilitas SDM dan governance (KPMG, 2024; Fortinet, 2024). Studi sistematis juga menekankan pentingnya integrasi kebijakan, latihan tabletop (drill), dan manajemen vendor sebagai bagian dari strategi yang efektif (Saeed, 2024). Namun, efektivitas setiap pendekatan dipengaruhi konteks organisasi, anggaran, dan tingkat kematangan teknologi.

Bukti empiris dan studi di sektor migas

Kajian literatur akademis (systematic reviews dan studi kasus) menunjukkan bahwa banyak penelitian fokus pada identifikasi ancaman, model risiko, dan solusi teknis (mis. intrusion detection untuk SCADA), sementara studi lapangan empiris yang mengukur *dampak* konkret intervensi *cyber security* terhadap indikator operasional (mis. downtime, frekuensi insiden, waktu pemulihan) masih relatif terbatas. Sebagai contoh, beberapa studi meninjau kasus-kasus besar (Colonial Pipeline, serangan pada fasilitas kilang) untuk menilai konsekuensi ekonomi dan regulasi, tetapi generalisasi ke konteks negara lain seringkali sulit dilakukan karena perbedaan struktur organisasi dan lingkungan regulasi (Saeed, 2024; ResearchGate systematic reviews 2024). Hal ini menunjukkan kebutuhan penelitian kuantitatif dan kualitatif yang lebih banyak pada level perusahaan migas.

Konteks Indonesia: regulasi, kesiapan, dan studi lokal

Di tingkat nasional, Badan Siber dan Sandi Negara (BSSN) aktif memonitor ancaman dan menerbitkan laporan yang menunjukkan potensi ancaman seperti ransomware, APT, dan serangan berbasis IoT (BSSN, 2023). Percepatan target produksi migas dan ekspansi operasi (Pertamina & Kebijakan ESDM) berimplikasi pada bertambahnya aset yang harus diamankan, sehingga menambah kompleksitas manajemen risiko siber (ESDM; Pertamina laporan/target produksi). Namun laporan-laporan domestik mengindikasikan adanya gap: keterbatasan SDM dengan kompetensi OT security, pembiayaan yang belum proporsional untuk OT, dan tantangan koordinasi antara regulator, operator, dan penyedia layanan keamanan (BSSN; reforminer/Reuters coverage on Pertamina targets). Kondisi ini menegaskan relevansi studi yang mengkaji dampak pendekatan *cyber security* secara kontekstual di Indonesia.

Evaluasi efektivitas pendekatan: metrik dan indikator

Literatur menyarankan indikator kombinasi teknis dan organisasi untuk menilai efektivitas: (1) indikator teknis, yaitu jumlah dan tingkat keparahan kerentanan yang tertutup, frekuensi

intrusi, waktu deteksi (MTTD) dan waktu respons (MTTR); (2) indikator operasional, yaitu frekuensi downtime produksi, durasi gangguan layanan, serta biaya pemulihan; (3) indikator organisasi, yaitu kepatuhan terhadap kebijakan, tingkat kesadaran karyawan, dan kesiapan latihan respons insiden. Namun, studi yang menghubungkan perubahan indikator-indikator ini secara kausal dengan implementasi pendekatan tertentu (mis. pemasangan IDS OT atau segmentasi jaringan) masih terbatas sehingga sulit menyimpulkan generalisasi efektivitas. Laporan KPMG dan Fortinet mengadvokasi pengukuran metrik terstandardisasi untuk membandingkan kemajuan, namun implementasinya beragam antar organisasi (KPMG, 2024; Fortinet, 2024).

B. Metodologi

Penelitian ini menggunakan pendekatan *mixed methods*, yaitu kombinasi metode kuantitatif dan kualitatif, untuk memperoleh gambaran yang menyeluruh mengenai dampak pendekatan *cyber security* terhadap pengamanan operasi industri migas di Indonesia. Metode kuantitatif dipilih untuk mengukur sejauh mana variabel penerapan *cyber security* berpengaruh terhadap tingkat pengamanan operasi, sedangkan metode kualitatif digunakan untuk memperdalam pemahaman tentang konteks, kendala, serta strategi implementasi yang ditemui di lapangan (Creswell & Plano Clark, 2018).

Data penelitian diperoleh dari dua sumber utama. Pertama, data primer yang dikumpulkan melalui penyebaran kuesioner kepada tenaga ahli, staf IT/OT security, serta manajer operasional di beberapa perusahaan migas yang beroperasi di Indonesia. Kuesioner ini menggunakan skala Likert untuk menilai tingkat penerapan kontrol *cyber security*, misalnya segmentasi jaringan, penggunaan sistem deteksi intrusi, manajemen patch, dan pelatihan kesadaran keamanan. Selain itu, penelitian ini juga melakukan wawancara mendalam dengan pihak kunci, termasuk pejabat regulator seperti BSSN atau SKK Migas, serta praktisi *cyber security* di sektor migas. Kedua, data sekunder diperoleh dari laporan tahunan perusahaan migas, laporan industri *cyber security* (Dragos, 2025; Fortinet, 2024; KPMG, 2024), serta regulasi pemerintah terkait keamanan infrastruktur kritis.

Populasi penelitian mencakup seluruh perusahaan migas yang beroperasi di Indonesia, baik BUMN maupun swasta. Namun, mengingat keterbatasan, penelitian ini menggunakan teknik *purposive sampling*, yaitu memilih perusahaan yang memiliki infrastruktur kritis berbasis OT/ICS, telah menerapkan kebijakan *cyber security*, dan bersedia memberikan data penelitian. Dari perusahaan-perusahaan tersebut, responden dipilih berdasarkan keterlibatan mereka dalam pengelolaan *cyber security* dan operasi, seperti manajer IT security, engineer OT/SCADA, manajer operasi lapangan, serta staf yang menangani risiko dan kepatuhan. Target jumlah responden kuesioner berkisar antara 100 hingga 150 orang, yang berasal dari perusahaan migas besar seperti Pertamina Group, Chevron Pacific Indonesia, dan Medco Energi, serta perusahaan skala menengah.

Proses pengumpulan data dilakukan melalui tiga teknik utama, yaitu kuesioner, wawancara, dan dokumentasi. Kuesioner digunakan untuk memperoleh data kuantitatif yang dapat diukur secara statistik. Wawancara dilakukan secara semi-terstruktur untuk menggali pengalaman praktis, kendala, dan strategi yang ditempuh dalam implementasi *cyber security*. Sementara itu, dokumentasi digunakan untuk menganalisis berbagai laporan insiden keamanan, laporan audit, serta kebijakan perusahaan yang relevan.

Instrumen penelitian berupa kuesioner dikembangkan berdasarkan indikator yang merujuk pada NIST Cybersecurity Framework (NIST, 2018) serta laporan industri terbaru (KPMG, 2024; Fortinet, 2024). Validitas isi instrumen diuji melalui konsultasi dengan pakar *cyber security* yang berpengalaman di bidang OT, sedangkan reliabilitasnya diuji menggunakan Cronbach's Alpha. Panduan wawancara disusun untuk melengkapi data kuantitatif dengan perspektif kualitatif yang lebih kontekstual.

Data yang terkumpul dianalisis dengan dua pendekatan. Analisis kuantitatif mencakup uji validitas dan reliabilitas instrumen, analisis deskriptif untuk menggambarkan tingkat penerapan *cyber security* dan kondisi pengamanan operasi, serta analisis regresi linier berganda untuk menguji pengaruh pendekatan *cyber security* terhadap pengamanan operasi migas. Selain itu, analisis korelasi digunakan untuk menilai hubungan antarvariabel. Di sisi lain, data kualitatif dari hasil wawancara dianalisis dengan metode *thematic analysis* guna mengidentifikasi tema-tema penting terkait kendala, praktik terbaik, dan rekomendasi kebijakan. Untuk menjamin validitas, dilakukan triangulasi antara data kuesioner, wawancara, dan dokumentasi.

Penelitian ini juga memperhatikan aspek etika, khususnya terkait kerahasiaan data responden dan perusahaan. Informasi yang diperoleh hanya digunakan untuk kepentingan akademis, dan hasil penelitian akan disajikan secara agregat tanpa menyebutkan nama individu maupun perusahaan secara langsung. Dengan metodologi ini, penelitian diharapkan mampu menghasilkan analisis yang komprehensif, tidak hanya mengenai efektivitas pendekatan *cyber security*, tetapi juga mengenai peluang perbaikan kebijakan dalam mendukung ketahanan energi nasional.

C. Hasil dan Pembahasan

Profil Ancaman Siber di Industri Migas Indonesia

Hasil analisis data kuesioner dan wawancara menunjukkan bahwa industri migas Indonesia menghadapi spektrum ancaman siber yang semakin kompleks, baik pada ranah teknologi informasi (IT) maupun teknologi operasional (OT). Sebagian besar responden, yaitu sekitar 82 persen, menekankan bahwa sistem operasi migas memiliki kerentanan tinggi terhadap serangan yang menyasar Industrial Control Systems (ICS) dan Supervisory Control and Data Acquisition (SCADA). Kerentanan ini terutama disebabkan oleh integrasi yang semakin erat antara IT dan OT, penggunaan perangkat keras lama yang tidak kompatibel dengan sistem keamanan modern, serta lemahnya segmentasi jaringan yang menyebabkan potensi eskalasi serangan dari sistem kantor ke sistem produksi (Kaspersky, 2023; Yaqoob et al., 2022).

Jenis serangan yang paling dominan diidentifikasi meliputi ransomware, phishing spear attacks, supply chain attacks, dan serangan terhadap perangkat Internet of Things (IoT) yang digunakan dalam monitoring lapangan migas. Ransomware menjadi perhatian utama karena memiliki kemampuan melumpuhkan sistem operasi kilang dan distribusi energi dalam waktu singkat (IBM Security, 2024). Dampaknya tidak hanya berupa kerugian finansial yang besar, tetapi juga hilangnya kepercayaan dari publik dan pemangku kepentingan. Sementara itu, phishing spear attacks umumnya menyasar staf teknis maupun manajerial untuk mencuri kredensial dan memanfaatkan akses tersebut guna menyusup ke sistem produksi (Verizon, 2024). Di sisi lain, serangan rantai pasok juga semakin marak, di mana kelemahan vendor perangkat lunak atau penyedia layanan pihak ketiga dapat dimanfaatkan sebagai pintu masuk serangan (ENISA, 2023). Serangan terhadap perangkat IoT pun menjadi ancaman serius, mengingat banyak sensor lapangan, drone inspeksi, dan perangkat monitoring cerdas belum dilengkapi dengan enkripsi maupun autentikasi yang memadai (NIST, 2022).

Jika dilihat dari tren insiden, sistem IT pada level kantor masih kerap menjadi sasaran malware infection, email spoofing, maupun pencurian data. Meski insiden ini mengganggu operasional administratif, dampaknya relatif dapat dipulihkan dengan mekanisme cadangan data. Namun, yang lebih dikhawatirkan adalah potensi penetrasi serangan dari IT menuju sistem OT. Serangan yang berhasil masuk ke ranah OT berisiko jauh lebih berbahaya karena dapat menyebabkan gangguan produksi, kerusakan peralatan bernilai tinggi, bahkan ancaman keselamatan kerja. Lebih jauh, gangguan pada sistem OT juga berpotensi menimbulkan pencemaran lingkungan apabila peralatan eksploitasi dan distribusi migas gagal berfungsi sebagaimana mestinya (He et al., 2021; World Economic Forum, 2024).

Temuan ini juga menegaskan bahwa ancaman siber yang dihadapi industri migas Indonesia tidak lagi sekadar bersifat teknis, tetapi juga strategis. Serangan siber tidak hanya menimbulkan kerugian berupa kehilangan data atau biaya pemulihan, melainkan juga mengancam ketahanan energi nasional. Sebuah serangan yang menargetkan kilang atau jaringan distribusi, misalnya, dapat berdampak langsung terhadap kelangkaan pasokan bahan bakar minyak dan gas domestik. Selain itu, insiden semacam ini akan merusak reputasi perusahaan, menurunkan kepercayaan investor, serta mengakibatkan kerugian ekonomi dalam skala besar (PwC, 2023). Lebih jauh lagi, karena migas merupakan bagian dari infrastruktur kritikal, ancaman siber juga dapat dimanfaatkan oleh aktor negara maupun kelompok kriminal terorganisir untuk melemahkan stabilitas ekonomi dan politik nasional (Rid, 2020).

Dalam konteks regional dan global, hasil penelitian ini sejalan dengan laporan Dragos (2025) yang mencatat peningkatan serangan siber pada sektor energi global sebesar 26 persen dibandingkan tahun sebelumnya. Asia Tenggara, termasuk Indonesia, tercatat sebagai salah satu kawasan yang paling banyak menjadi sasaran. Hal ini memperkuat pandangan bahwa industri migas Indonesia merupakan target yang menarik, baik bagi kelompok kriminal siber yang berorientasi finansial, hacktivist yang ingin melumpuhkan infrastruktur penting, maupun aktor negara yang memiliki kepentingan geopolitik dan energi (Dragos, 2025; ICS-CERT, 2023). Dengan demikian, profil ancaman siber yang dihadapi sektor migas Indonesia menuntut perhatian serius,

karena dampaknya tidak hanya terbatas pada ranah operasional, tetapi juga mencakup dimensi strategis yang menyangkut ketahanan energi dan keamanan nasional.

Pendekatan *Cyber Security* yang Diterapkan

Hasil penelitian juga menunjukkan bahwa sebagian besar perusahaan migas besar di Indonesia, seperti Pertamina Group dan Medco Energi, telah mengadopsi kerangka kerja *cyber security* berbasis standar internasional, di antaranya NIST Cybersecurity Framework dan ISO/IEC 27001. Kerangka kerja ini memberikan landasan yang kuat bagi penerapan kontrol teknis, administratif, maupun prosedural untuk melindungi aset digital dan operasional. Penerapan standar global tersebut mencerminkan kesadaran industri migas nasional terhadap tingginya risiko serangan siber, terutama pada sektor energi yang dikategorikan sebagai infrastruktur kritikal (ISO, 2018; NIST, 2020).

Dari hasil kuesioner, tercatat 76% responden menyatakan bahwa perusahaan mereka telah melakukan segmentasi jaringan antara sistem IT dan OT sebagai langkah pencegahan utama untuk mengurangi kemungkinan eskalasi serangan. Selain itu, 68% perusahaan telah mengimplementasikan *intrusion detection system* (IDS) khusus pada jaringan OT guna mendeteksi aktivitas mencurigakan sebelum berdampak lebih luas. Sementara itu, 72% responden melaporkan bahwa patch management pada sistem kritis dilakukan secara rutin untuk menutup celah kerentanan perangkat lunak. Praktik-praktik ini menunjukkan adanya pergeseran dari pendekatan keamanan reaktif menuju proaktif, di mana perlindungan dilakukan sebelum insiden terjadi, bukan hanya setelah serangan berlangsung (ENISA, 2023).

Selain kontrol teknis, perusahaan migas besar di Indonesia juga mulai menaruh perhatian lebih pada aspek sumber daya manusia. Data survei menunjukkan bahwa 65% responden melaporkan pelatihan kesadaran *cyber security* dilakukan minimal dua kali setahun. Pelatihan ini bertujuan meningkatkan kewaspadaan karyawan terhadap ancaman seperti *phishing*, *social engineering*, dan kesalahan manusia yang sering menjadi pintu masuk serangan. Meski demikian, wawancara dengan beberapa informan mengungkapkan bahwa tantangan terbesar terletak pada unit operasi lapangan di lokasi terpencil, di mana akses terhadap pelatihan masih belum konsisten. Hal ini sejalan dengan temuan sebelumnya bahwa faktor manusia tetap menjadi titik lemah utama dalam sistem pertahanan siber, meskipun infrastruktur teknis telah diperkuat (Verizon, 2024).

Pendekatan lain yang mulai diadopsi adalah pemanfaatan teknologi *threat intelligence* untuk memantau pola serangan secara real-time. Wawancara dengan salah satu manajer IT security di perusahaan migas BUMN menunjukkan bahwa kerja sama dengan Badan Siber dan Sandi Negara (BSSN) serta penyedia intelijen ancaman internasional membantu perusahaan dalam mengidentifikasi potensi serangan sejak dini. Kolaborasi lintas lembaga ini memungkinkan perusahaan memperoleh peringatan dini (*early warning*) terhadap serangan siber, sehingga mitigasi dapat dilakukan lebih cepat sebelum menimbulkan kerugian yang signifikan. Studi terdahulu juga menekankan pentingnya integrasi threat intelligence dalam strategi *cyber security* industri energi, karena ancaman sering kali bersifat global dan terkoordinasi lintas negara (Dragos, 2025; IBM Security, 2024).

Namun demikian, implementasi strategi *cyber security* di sektor migas Indonesia masih menunjukkan variasi yang cukup signifikan. Perusahaan besar dengan sumber daya memadai cenderung mampu mengadopsi pendekatan komprehensif dan proaktif. Sebaliknya, perusahaan migas skala menengah dan kecil menghadapi keterbatasan baik dari segi teknologi maupun tenaga ahli. Akibatnya, mereka lebih banyak mengandalkan pendekatan reaktif, yakni menanggapi serangan setelah terjadi, daripada membangun sistem pertahanan yang mampu mencegah serangan sejak awal. Ketimpangan ini menjadi catatan penting dalam upaya memperkuat ketahanan siber sektor energi secara nasional, karena kerentanan pada satu entitas dapat berimplikasi pada rantai pasok energi secara keseluruhan (PwC, 2023; Rid, 2020).

Dampak Penerapan *Cyber Security* terhadap Pengamanan Operasi

Hasil penelitian memperlihatkan bahwa penerapan kontrol *cyber security* dalam industri migas tidak hanya menghasilkan perlindungan teknis, tetapi juga membentuk budaya baru dalam menjaga keberlangsungan operasi. Segmentasi jaringan, sistem deteksi intrusi, manajemen patch, dan pelatihan kesadaran keamanan terbukti menciptakan lapisan pertahanan yang membuat organisasi lebih tangguh menghadapi serangan siber (ISO, 2018; NIST, 2020). Perusahaan yang konsisten dalam mengimplementasikan praktik-praktik ini menunjukkan tingkat kesiapan yang lebih baik, sehingga mampu mengendalikan potensi gangguan dengan cara yang lebih cepat dan terukur (ENISA, 2023; Kaspersky, 2023).

Wawancara dengan praktisi keamanan di perusahaan migas BUMN, misalnya, menegaskan bahwa penerapan sistem pemantauan intrusi secara real-time telah memberikan perbedaan nyata. Mereka menggambarkan bagaimana insiden yang dulunya sering mengganggu kelancaran produksi kini dapat dicegah sejak dini, bahkan sebelum menimbulkan dampak signifikan. Lebih jauh, responden menjelaskan bahwa salah satu perubahan yang paling dirasakan bukan hanya berkurangnya jumlah serangan yang berhasil, melainkan meningkatnya rasa percaya diri tim operasi dalam menjalankan tugas sehari-hari (Dragos, 2025; IBM Security, 2024).

Peningkatan ini juga terlihat pada aspek pemulihan. Jika sebelumnya gangguan siber dapat menyebabkan terhentinya produksi selama berjam-jam, kini waktu pemulihan menjadi jauh lebih singkat. Hal ini menumbuhkan keyakinan bahwa *cyber security* bukan sekadar teknologi tambahan, tetapi merupakan fondasi yang menopang kelangsungan bisnis. Pandangan tersebut diperkuat oleh pemahaman baru di kalangan manajemen, bahwa investasi pada keamanan digital sama pentingnya dengan investasi pada peralatan produksi atau infrastruktur fisik lainnya (KPMG, 2024; PwC, 2023).

Dengan demikian, penelitian ini menegaskan bahwa *cyber security* di sektor migas bukanlah isu teknis belaka. Lebih dari itu, ia merupakan strategi keberlanjutan yang menjaga keandalan operasi sekaligus ketahanan energi nasional. Perusahaan yang berhasil mengintegrasikan kontrol *cyber security* ke dalam sistem kerjanya tidak hanya mengurangi risiko insiden, tetapi juga menciptakan ekosistem kerja yang lebih resilien, adaptif, dan siap menghadapi dinamika ancaman global yang terus berkembang (World Economic Forum, 2024; Yaqoob et al., 2022).

Kendala dalam Implementasi *Cyber security*

Meskipun penerapan berbagai kontrol *cyber security* memberikan dampak positif bagi keberlanjutan operasi, terdapat sejumlah kendala yang signifikan dalam implementasinya di sektor migas Indonesia. Kendala pertama terletak pada keterbatasan sumber daya manusia (SDM) yang memiliki kompetensi khusus di bidang keamanan sistem operasi industri (OT). Berdasarkan hasil kuesioner, sekitar 71% responden menyatakan bahwa jumlah tenaga ahli yang memahami integrasi IT–OT masih sangat terbatas. Akibatnya, perusahaan sering kali bergantung pada konsultan eksternal untuk menangani aspek teknis kritis, yang dalam jangka panjang dapat menimbulkan ketergantungan dan meningkatkan biaya operasional (Dragos, 2025; Yaqoob et al., 2022).

Kendala kedua berkaitan dengan aspek regulasi dan koordinasi antarinstansi. Meskipun Badan Siber dan Sandi Negara (BSSN) serta SKK Migas telah menginisiasi sejumlah pedoman dan program peningkatan kapasitas, responden menilai bahwa regulasi yang ada masih bersifat umum dan belum sepenuhnya mengakomodasi kebutuhan spesifik industri migas. Fragmentasi regulasi ini sering menyebabkan kebingungan di tingkat implementasi, terutama ketika perusahaan harus menyesuaikan standar internasional seperti NIST Cybersecurity Framework atau ISO/IEC 27001 dengan kebijakan nasional yang berlaku (NIST, 2020; ISO, 2018).

Kendala berikutnya adalah biaya investasi yang tinggi. Perusahaan migas skala menengah, yang memiliki keterbatasan modal, menghadapi kesulitan dalam membiayai teknologi keamanan mutakhir, seperti Security Information and Event Management (SIEM) atau sistem deteksi intrusi berbasis kecerdasan buatan. Kondisi ini memaksa mereka untuk memilih solusi minimalis dengan efektivitas terbatas. Padahal, literatur menunjukkan bahwa organisasi yang hanya mengandalkan pendekatan reaktif tanpa dukungan sistem keamanan proaktif berisiko lebih tinggi mengalami eskalasi serangan dengan dampak yang lebih parah (Kaspersky, 2023; IBM Security, 2024).

Selain faktor teknis dan finansial, budaya organisasi juga menjadi salah satu penghambat utama. Wawancara dengan seorang manajer operasional di salah satu perusahaan migas BUMN mengungkapkan bahwa sebagian pekerja lapangan masih menganggap *cyber security* sebagai isu sekunder dibandingkan keselamatan fisik (safety). Padahal, serangan terhadap sistem kontrol industri, seperti SCADA atau ICS, dapat berdampak langsung terhadap keselamatan kerja maupun kerusakan peralatan vital (ENISA, 2023; PwC, 2023). Rendahnya kesadaran ini menunjukkan bahwa transformasi budaya organisasi dalam memandang *cyber security* sebagai bagian integral dari keselamatan dan keberlanjutan operasi masih menjadi pekerjaan rumah besar bagi industri migas di Indonesia.

Jawaban atas Pertanyaan Penelitian

Berdasarkan hasil analisis, pertanyaan penelitian dapat dijawab sebagai berikut:

1. Bagaimana profil ancaman siber yang dihadapi industri migas di Indonesia? Ancaman utama berupa serangan terhadap sistem OT/ICS, dengan modus *ransomware*,

phishing, dan *supply chain attack* yang berpotensi mengganggu produksi dan keselamatan kerja.
2. Apa saja pendekatan *cyber security* yang telah diterapkan dalam operasi migas? Perusahaan migas besar telah menerapkan segmentasi jaringan, IDS, manajemen patch, awareness training, serta *threat intelligence*. Namun, perusahaan skala menengah masih menghadapi keterbatasan dalam adopsi.
3. Sejauh mana pendekatan tersebut berdampak pada pengamanan operasi migas di Indonesia? Penerapan *cyber security* terbukti menurunkan frekuensi insiden, mempercepat waktu pemulihan, dan meningkatkan keandalan operasi. Dampaknya signifikan terhadap keberlanjutan operasi dan ketahanan energi nasional.
4. Apa kendala utama dalam implementasi *cyber security* di sektor migas? Kendala meliputi keterbatasan SDM, fragmentasi regulasi, tingginya biaya investasi, serta budaya organisasi yang belum sepenuhnya mendukung *cyber security*.

Temuan penelitian ini menegaskan bahwa pendekatan *cyber security* dalam industri migas Indonesia belum bisa dianggap sebagai opsi tambahan, melainkan kebutuhan mendesak. Hal ini sejalan dengan tren global yang menempatkan sektor energi sebagai infrastruktur kritis dengan tingkat ancaman tinggi (World Economic Forum, 2024). Namun demikian, penerapan *cyber security* masih menghadapi kesenjangan antara perusahaan besar dan menengah. Kesenjangan ini berpotensi menimbulkan kerentanan sistemik, karena rantai pasok migas saling terhubung. Oleh karena itu, kolaborasi antara pemerintah, perusahaan besar, dan perusahaan skala menengah menjadi penting untuk menciptakan ekosistem *cyber security* yang lebih tangguh. Penelitian ini juga membuka ruang bagi kajian lanjutan. Misalnya, studi perbandingan antara sektor migas di Indonesia dengan negara lain di kawasan ASEAN dapat memberikan wawasan baru mengenai praktik terbaik (best practices) yang relevan untuk diadopsi.

D. Kesimpulan

Penelitian ini menemukan bahwa industri migas Indonesia menghadapi ancaman siber yang semakin kompleks, terutama pada sistem OT/ICS yang berpotensi mengganggu produksi dan keselamatan kerja. Pendekatan *cyber security* yang diterapkan, seperti segmentasi jaringan, IDS, manajemen patch, pelatihan kesadaran, dan *threat intelligence*, terbukti berpengaruh positif terhadap pengamanan operasi dengan menekan frekuensi insiden, mempercepat pemulihan, serta meningkatkan keandalan produksi.

Temuan ini menegaskan bahwa *cyber security* merupakan investasi strategis bagi industri migas, bukan sekadar biaya tambahan. Dari sisi akademis, penelitian ini memperkaya kajian tentang *cyber security* di sektor energi negara berkembang. Dari sisi praktis, hasil penelitian dapat menjadi dasar bagi pemerintah, khususnya BSSN dan SKK Migas, untuk memperkuat regulasi dan pedoman *cyber security* yang lebih spesifik bagi sektor migas, serta bagi perusahaan untuk meningkatkan kapasitas SDM dan memperluas kolaborasi lintas sektor.

Penelitian ini memiliki keterbatasan pada cakupan sampel yang masih terbatas, ketergantungan pada data persepsi responden, serta dinamika ancaman siber yang cepat berubah. Hal ini membuat hasil penelitian perlu diperbarui secara berkala dan diperkaya dengan studi yang lebih luas, baik dari sisi jumlah perusahaan yang terlibat maupun perbandingan dengan sektor energi di negara lain.

Untuk memperkuat *cyber security* sektor migas, perusahaan perlu mengadopsi strategi yang lebih proaktif, termasuk pemanfaatan teknologi berbasis kecerdasan buatan untuk deteksi dini serangan. Pemerintah disarankan mempercepat harmonisasi regulasi dan menetapkan standar minimum *cyber security* bagi sektor migas. Penelitian selanjutnya sebaiknya melibatkan lebih banyak perusahaan, termasuk penyedia jasa penunjang migas, serta mengembangkan studi komparatif di tingkat regional agar diperoleh gambaran yang lebih komprehensif.

E. Referensi

Automation.com. (2024). *Cybersecurity in the Oil and Gas Industry: Challenges and Strategies*. Automation.com.

Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan Cyber security Nasional*. Jakarta: BSSN.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

Dragos. (2025). *OT Cybersecurity Year in Review 2024*. Dragos Inc.

ENISA. (2023). *Threat landscape for industrial control systems*. European Union Agency for Cybersecurity.

Fortinet. (2024). *Securing Operational Technology in Oil and Gas*. Fortinet Research Report.

Healy, P. M., & Wahlen, J. M. (1999). A review of the earnings management literature and its implications for standard setting. *Accounting Horizons, 13*(4), 365–383.

IBM Security. (2024). *X-Force threat intelligence index 2024*. IBM Security.

ISO. (2018). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.

Kaspersky. (2023). *OT/ICS cybersecurity report 2023*. Kaspersky Lab.

KPMG. (2024). *Cyber security as a business enabler in the energy sector*. KPMG International.

KPMG. (2024). *ICS/OT Cybersecurity Report 2024*. KPMG International.

Lee, R., Assante, M., & Conway, T. (2022). *Industrial Cybersecurity Case Studies: Lessons Learned from Real Attacks*. SANS Institute.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://www.nist.gov/cyberframework

NIST. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). National Institute of Standards and Technology.

Pertamina. (2024). *Rencana Strategis Hulu Migas 2024–2030*. PT Pertamina (Persero).

PwC. (2023). *Global digital trust insights: Securing critical infrastructure*. PricewaterhouseCoopers.

Reuters. (2024, June 24). *Indonesia hit by major ransomware attack on national data center*. Reuters.

World Economic Forum. (2024). *Global risks report 2024*. World Economic Forum.

World Economic Forum. (2024). *Global risks report 2024*. World Economic Forum. https://www.weforum.org

Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y., Al-Garadi, M. A., & Omar, M. (2022). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Future Generation Computer Systems, 126,* 169–190.