

## **MENGELOLA OBJEK VITAL, PENGAMANAN FILE, DAN PENGAMANAN *CYBER* TERHADAP MANAJEMEN SEKURITI PADA PT. PERTAMINA (PERSERO)**

**Edy Soesanto\***

Program Studi Teknik Perminyakan, Universitas Bhayangkara Jakarta Raya  
[edysoesanto@dsn.ubharajaya.ac.id](mailto:edysoesanto@dsn.ubharajaya.ac.id)

**Anna Wijayanti**

Ekonomi & Bisnis/Manajemen, Universitas Bhayangkara Jakarta Raya

**Muhamad Elzan Musyafa**

Ekonomi & Bisnis/Manajemen, Universitas Bhayangkara Jakarta Raya

**Nurul Cahyani**

Ekonomi & Bisnis/Manajemen, Universitas Bhayangkara Jakarta Raya

### **ABSTRAK**

PT. Pertamina (Persero) adalah satu satunya BUMN (Badan Usaha Milik Negara) yang bergerak dalam bidang usaha minyak dan gas terintegrasi, mulai dari lingkup kerja hulu hingga hilir dengan aset yang sangat banyak perlu dijaga. PT Pertamina (Persero) memastikan pemenuhan kebutuhan BBM dan LPG serta pelayanan ke masyarakat akan tetap menjadi prioritas utama Perusahaan. Sebagai BUMN, Pertamina termasuk seluruh pekerja bertanggung jawab dalam menjalankan amanah Pemerintah untuk memastikan ketahanan energi nasional. Tujuan dari penelitian ini adalah untuk mengetahui objek vital, pengamanan file, dan pengamanan cyber terhadap manajemen sekuriti pada PT. Pertamina (Persero). metode penelitian ini menggunakan penelitian kualitatif dengan pendekatan *Systematic Review*, sumber data yang digunakan pada penelitian ini adalah data Sekunder yaitu data yang diperoleh atau dikumpulkan peneliti dari berbagai sumber yang telah ada. Data sekunder dapat berupa data dari Annual Report PT. Pertamina (Persero) dan sebagainya. Hasil penelitian pada jurnal ini Sebagai bahan informasi tambahan dan masukan bagi Perusahaan yang dapat dijadikan pertimbangan dalam mengelola Objek Vital, Pengamanan File dan Pengamanan *Cyber* terhadap Manajemen Sekuriti pada PT. Pertamina (Persero), seperti halnya pembangunan proyek konstruksi resiko kecelakaan kerja yang menjadi terganggunya aktivitas pekerja proyek tersebut.

**Kata Kunci: Mengelola Objek Vital, Pengamanan File, Pengamanan Cyber, PT. Pertamina**

### ***ABSTRACT***

*PT. Pertamina (Persero) is the only BUMN (State Owned Enterprise) engaged in the integrated oil and gas business, starting from the upstream to downstream scope of work with assets that really need to be maintained. PT Pertamina (Persero) ensures that meeting the needs for fuel*

*and LPG as well as providing services to the community remain the Company's main priorities. As a BUMN, Pertamina, including all workers, is responsible for carrying out the Government's mandate to ensure national energy security. The purpose of this study is to determine vital objects, file security, and cyber security against security management at PT. Pertamina (Persero). This research method uses qualitative research with a Systematic Review approach, the source of data used in this study is secondary data, namely data obtained or collected by researchers from various existing sources. Secondary data can be in the form of data from the Annual Report of PT. Pertamina (Persero) and so on. The results of research in this journal serve as additional information material and input for companies that can be taken into consideration in managing Vital Objects, File Security and Cyber Security for Security Management at PT. Pertamina (Persero), as with construction projects, the risk of work accidents disrupts the activities of the project workers.*

**Keywords: Manage Vital Objects, File Protection, Cyber Security, PT. Pertamina**

## **PENDAHULUAN**

PT. Pertamina (Persero) adalah satu-satunya BUMN (Badan Usaha Milik Negara) yang bergerak dalam bidang usaha minyak dan gas terintegrasi, mulai dari lingkup kerja hulu hingga hilir dengan aset yang sangat banyak perlu dijaga. Hal tersebut membuat PT. Pertamina termasuk kedalam salah satu Objek Vital Nasional (Obvitnas) Bidang Energi dan Sumber Daya Mineral. Peraturan Menteri Energi dan Sumber Daya Mineral Republik Indonesia Bab I pasal 1 menyebutkan bahwa, “Objek Vital Nasional Bidang Energi dan Sumber Daya Mineral yang selanjutnya disebut Obvitnas Bidang ESDM adalah kawasan/lokasi, bangunan/instalasi, dan/atau usaha yang menyangkut hajat hidup orang banyak, kepentingan negara dan/atau sumber pendapatan negara yang bersifat strategis di bidang energi dan sumber daya mineral”. Dalam pembangunan proyek konstruksi risiko kecelakaan kerja seringkali terjadi.

Kecelakaan kerja dapat menjadi salah satu penyebab terganggunya aktivitas pekerjaan proyek. Untuk itu perlu perhatian khusus dalam menangani kasus tersebut. Penerapan Sistem Manajemen Keselamatan dan Kesehatan Kerja (SMK3) yang baik dapat meminimalisir kemungkinan risiko kecelakaan kerja yang terjadi. Dalam penerapan SMK3 tersebut meliputi analisis risiko, memberi penilaian serta pengendalian risiko. Sehubungan dengan rencana mogok kerja yang dilayangkan Forum Serikat Pekerja Pertamina Bersatu (FSPBB), PT Pertamina (Persero) memastikan pemenuhan kebutuhan BBM dan LPG serta pelayanan ke masyarakat akan tetap menjadi prioritas utama Perusahaan. Sebagai BUMN, Pertamina termasuk seluruh pekerja bertanggung jawab dalam menjalankan amanah Pemerintah untuk memastikan ketahanan energi nasional. Pekerja juga menjadi garda terdepan dalam pelayanan kepada masyarakat dan menjalankan penugasan Pemerintah untuk memenuhi kebutuhan BBM dan LPG hingga ke pelosok wilayah 3T agar masyarakat terus dapat beraktivitas. Terlebih saat ini, Indonesia sedang berjuang keluar dari pandemi Covid-19 sehingga roda perekonomian nasional harus terus didorong bergerak.

Manajemen PT. Pertamina juga akan mengoptimalkan antisipasi dan mitigasi pada kondisi apapun untuk memastikan operasional perusahaan tetap dapat berjalan lancar dan pelayanan BBM dan LPG tidak mengalami gangguan. Berdasarkan Keputusan Presiden (Keppres) No. 63 Tahun 2004, infrastruktur energi yang berada di wilayah operasi Pertamina merupakan Objek Vital Nasional (Obvitnas) yang harus terbebas dari ancaman dan gangguan. Sesuai

Keppres tersebut, ancaman dapat dimaknai sebagai setiap usaha dan kegiatan dengan segala bentuknya baik yang berasal dari dalam negeri maupun luar negeri yang dinilai dapat berpotensi membahayakan kelangsungan berfungsinya Obvitnas. Sedangkan gangguan adalah tindakan yang sudah nyata dan menimbulkan kerugian berupa korban jiwa dan atau harta benda serta dapat berakibat trauma psikis kepada pegawai karyawan Obvitnas. *Vice President Corporate Communication* Pertamina, Fajriyah Usman menjelaskan Pertamina sebagai perusahaan yang mengelola energi nasional bertanggung jawab dalam memastikan keamanan infrastruktur termasuk usaha, kawasan atau lokasi, bangunan atau instalasi energi yang merupakan hajat hidup orang banyak, kepentingan negara dan atau sumber pendapatan negara yang bersifat strategis.

Untuk itu, kami berharap seluruh pekerja PT. Pertamina ikut bertanggung jawab dalam mengamankan Obvitnas di area operasi dan menjauhkan dari segala ancaman dan gangguan sebagai bentuk kontribusi kita pada bangsa dan negara, mengingat kawasan, infrastruktur dan instalasi energi tersebut sangat diperlukan untuk melayani kebutuhan energi di seluruh wilayah Indonesia. Dalam rangka mewujudkan keamanan dan kedaulatan energi, Pertamina berfokus menerapkan *best-in-class Security Management System* berbasis pengelolaan risiko. Pengelolaan keamanan dilakukan dengan berbasis Pertamina *Security Risk Management* (PSRM). PSRM mengatur mekanisme penyusunan profil risiko, pemantauan risiko keamanan, implementasi mitigasi risiko, serta pembaruan *security risk register*. PSRM membantu dalam mengambil keputusan di seluruh lingkungan korporat Pertamina berdasarkan prinsip manajemen risiko. Sejalan dengan transformasi digital, Pertamina berkomitmen selalu meningkatkan keamanan siber, keamanan transaksi elektronik dan keamanan digital lainnya. Pertamina bersama dua institusi Penyelenggara Sertifikat Elektronik (PSE) telah bekerja sama dalam pemanfaatan tanda tangan elektronik.

Pemanfaatan ini dilaksanakan khususnya pada penerbitan *invoice* dari *core system ERP* di Holding, maupun kegiatan penandatanganan dokumen elektronik korespondensi eksternal oleh para pekerja di Pertamina. Pasal 28 PM Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam sistem elektronik. Setiap Penyelenggara Sistem Elektronik wajib memberitahukan secara tertulis kepada pemilik data pribadi jika terjadi kegagalan perlindungan rahasia data pribadi dalam sistem elektronik yang dikelolanya. Kebijakan teknis keamanan *cyber* sehingga dapat memperkuat keamanan dan keandalan sistem elektronik PSE dalam kegiatan pemrosesan data pribadi yang diatur oleh Badan Siber dan Sandi Negara (BSSN). BSSN adalah Lembaga yang berwenang diantaranya untuk merumuskan kebijakan teknis keamanan *cyber* dan bertugas untuk melakukan manajemen risiko keamanan *cyber* sistem elektronik sesuai amanat PP PSTE dan Pepses No. 28 Tahun 2021 tentang BSSN.

Berdasarkan uraian diatas, maka pembahasan dalam artikel ini ialah “Mengelola Objek Vital, Pengamanan File, dan Pengamanan *Cyber* Terhadap Manajemen Sekuriti pada PT. Pertamina (Persero).”

## **LANDASAN TEORI**

### **Mengelola Objek Vital Nasional pada PT. Pertamina (Persero)**

Mengelola Objek Vital Nasional mempunyai peran yang cukup penting dalam pembangunan nasional. Di lain pihak, dimensi ancaman dan gangguan keamanan semakin

berkembang dengan beragam risiko dan dampaknya. Ancaman dan gangguan keamanan terhadap Obyek Vital Nasional secara langsung maupun tidak langsung berdampak pada sistem perekonomian nasional, stabilitas politik, serta keamanan nasional. PT. Pertamina (Persero) mempunyai Objek Vital Nasional (Obvitnas) yang harus terbebas dari ancaman dan juga kendala. Menurut (Rahayu et al., 2023). PT. Pertamina merupakan kilang minyak yang dapat dijadikan suatu Objek Vital Nasional, sebab perusahaan tersebut dapat memenuhi hajat hidup orang banyak dan kepentingan negeri serta sumber pemasukan negeri yang strategis.

Pengelolaan obvitnas disektor energi yang dikelola PT. Pertamina (Persero) seperti aset hulu migas, geothermal, kilang minyak, terminal BBM, hingga SPBU yang dipakai untuk menyalurkan kebutuhan BBM nasional. Dalam hal ini, baik TNI maupun Polri telah melaksanakan kerja-sama dengan PT. Pertamina (Persero), dimana penandatanganan dilakukan antara Direktur Utama PT. Pertamina dengan Panglima TNI dan Kapolri. Nota kesepahaman ini dimaksudkan guna mengatur kerjasama antara TNI/Polri dan PT. Pertamina (Persero) dalam upaya pengelolaan obvitnas, khususnya aset operasional, produksi dan distribusi BBM. PT. Pertamina (Persero) Terminal BBM dijadikan kawasan Obvitnas karena memiliki aset-aset strategis seperti aset-aset hulu migas dan geothermal, kilang minyak (tangi timbun) yang berjumlah 17 unit dengan rincian 4 tangki timbun premium, 2 tangki timbun korosene, 6 tangki timbun solar, 2 tangki timbun pertamax dan 3 tangki timbun avtur. Kemudian terdapat Filling Shed berjumlah 13 unit dengan rincian 3 Filling Shed premium, 3 Filling Shed korosene, 5 Filling Shed solar, 1 Filling Shed pertamax dan 1 Filling Shed avtur. Sedangkan dermaga untuk bersandar kapal tanker berjumlah 3 dermaga. PT. Pertamina (Persero) memastikan bahwa pemenuhan kebutuhan BBM dan LPG, serta memberikan pelayanan kepada masyarakat tetap menjadi prioritas utama Perusahaan.

PT. Pertamina merupakan Objek Vital Nasional (Obvitnas) yang harus bebas dari ancaman dan gangguan. (*Vice President Corporate Communication*) untuk itu PT. Pertamina, dan seluruh insan masyarakat harus turut serta bertanggung jawab dalam mengamankan Obvitnas di wilayah operasi, menjauhi segala ancaman dan gangguan sebagai bentuk kontribusi kepada bangsa dan negara, mengingat letaknya infrastruktur dan instalasi energi sangat dibutuhkan untuk melayani kebutuhan energi di seluruh wilayah Indonesia. PT. Pertamina (Persero) juga memiliki berbagai kebijakan dan prosedur dalam mengelola keamanan untuk menjaga kilang minyak sebagai Objek Vital Nasional (Obvitnas) mereka, yaitu dengan cara sebagai berikut:

1. Menggunakan teknologi keamanan seperti kamera pengawas, sistem alarm, dan pengamanan fisik seperti pagar dan gerbang.
2. Selain itu, PT. Pertamina juga menerapkan prosedur keamanan yang ketat untuk mengatur akses ke area kilang minyak dan memastikan bahwa hanya orang yang berwenang yang dapat memasuki area tersebut.
3. Serta semua karyawan PT. Pertamina yang diwajibkan untuk mengikuti pelatihan keamanan dan mematuhi protokol keamanan yang telah ditetapkan oleh perusahaan.

### **Pengamanan File pada PT. Pertamina (Persero)**

Pengamanan file adalah aksi penangkalan dari serbuan pengguna file atau pengakses jaringan yang tidak bertanggung jawab. Menurut (Ian, 2017) Keamanan sistem merupakan penilaian, sejauh mana sistem dapat melindungi suatu file dari serangan eksternal yang

mungkin sengaja ataupun tidak sengaja, seperti virus. Pada suatu Perusahaan seperti PT. Pertamina sistem keamanan file untuk data informasi elektronik menjadi suatu hal yang sangat penting bagi perusahaan yang menggunakan fasilitas IT dan menempatkannya sebagai infrastruktur. Karena data merupakan informasi ataupun asset bagi perusahaan tersebut. Setiap data pribadi yang telah dikumpulkan di situs MyPertamina diperuntukkan kepada PT. Pertamina (Persero) sendiri. Berbagai cara yang diterapkan Perusahaan PT. Pertamina dalam mengamankan aplikasi MyPertamina untuk mencegah terjadinya insiden hacking di masa depan. Berikut ini ialah beberapa langkah-langkah umum yang diterapkan PT. Pertamina untuk mengamankan aplikasi MyPertamina, yaitu sebagai berikut:

1. Melakukan audit keamanan  
Langkah ini melibatkan penilaian dalam mengidentifikasi kerentanan potensial aplikasi (MyPertamina) dan mengatasi keamanan aplikasi sebelum dimanfaatkan oleh peretas.
2. Implementasi otentikasi multi-faktor  
Cara ini digunakan untuk menambahkan lapisan keamanan tambahan dengan mengharuskannya pengguna dalam memberikan informasi tambahan, seperti halnya tambahan kata sandi untuk mengakses aplikasi MyPertamina.
3. Menggunakan enkripsi  
Enkripsi ini dapat membantu melindungi data sensitif dengan mengubahnya menjadi kode yang hanya dapat didekripsi dengan kunci.
4. Perbarui aplikasi secara teratur  
Meng-*update* aplikasi MyPertamina dapat memastikan bahwa setiap patch keamanan atau pembaruan diinstal untuk mengatasi kerentanan yang diketahui.
5. Pelatihan Karyawan (*Training*)  
Pelatihan karyawan ialah praktik setiap keamanan perusahaan, agar pekerja dapat membantu mencegah mereka yang secara tidak sengaja mengekspos aplikasi ke ancaman potensial.

### **Pengamanan *Cyber* pada PT. Pertamina (Persero)**

Dikutip dari (Institut Teknologi Sepuluh Nopember, 2023) Keamanan Siber atau *Cyber Security* adalah praktik untuk melindungi sistem, jaringan, dan program dari serangan digital. Serangan-serangan ini biasanya ditujukan untuk mengakses, mengubah, atau menghancurkan informasi sensitive, serta memeras uang dari pengguna. Menerapkan langkah-langkah *cyber security* yang efektif sangat menantang, karena ada lebih banyak perangkat dibandingkan dengan manusianya, dan penyerang menjadi lebih inovatif. *Cyber attack* atau serangan *cyber* pada era digital saat ini menjadi sebuah persoalan yang tidak dapat dihindari.

PT. Pertamina melalui fungsi Enterprise IT terus memberikan sosialisasi mengenai pentingnya memperkuat keamanan pada sistem digital setiap orang. SVP Enterprise IT Pertamina mengatakan, kegiatan sosialisasi mengenai *cyber attack* ini memiliki tujuan untuk memberikan kesadaran kepada para pekerja ataupun TKJP (Penyediaan Tenaga Kerja Jasa Penunjang) dan seluruh orang yang berada dalam naungan PT. Pertamina (Persero) pada aspek *cyber security* atau *security information*. PT. Pertamina berharap seluruh pekerja, TKJP hingga mitra kerja yang berada di lingkungan PT. Pertamina bisa memiliki kesadaran terhadap keamanan *cyber*. Sebab, keamanan *cyber* menjadi salah satu aspek yang dipantau oleh ESG. Sejalan dengan transformasi digital yang berkembang saat ini PT. Pertamina (Persero)

berkomitmen untuk meningkatkan keamanan *cyber*nya, keamanan transaksi elektronik serta keamanan digital yang lain.

PT. Pertamina bersama 2 institusi Penyelenggara Sertifikat Elektronik (PSE) sudah bekerja sama dalam pemanfaatan ciri tangan elektronik. Pemanfaatan ini dilaksanakan spesialnya pada penerbitan invoice dari *core system* ERP di Holding, ataupun aktivitas penandatanganan dokumen elektronik korespondensi eksternal oleh para pekerja di PT. Pertamina. Pengamanan *cyber* merupakan masalah yang krusial bagi perusahaan seperti PT. Pertamina, mengingat pentingnya infrastruktur dan data yang mereka kelola. Berikut ini ialah contoh penerapan pengamanan *cyber* pada PT. Pertamina (Persero) yaitu:

1. PT. Pertamina (Persero) memiliki kode perilaku yang memastikan semua dokumen lengkap, mencerminkan kondisi aktual, akurat, tepat waktu, dapat dilacak sampai transaksi, dan aman.
2. PT. Pertamina (Persero) memiliki kebijakan privasi yang menjelaskan cara mereka mengumpulkan, menyimpan, menggunakan, dan melindungi informasi yang dapat dikaitkan dengan orang fisik atau hukum tertentu.
3. PT. Pertamina (Persero) memiliki kode pemerintahan yang mencakup manajemen aset, yang meliputi pengadaan, pemanfaatan, pemeliharaan, keamanan, serta pemecahan masalah.

### **Manajemen Sekuriti**

Manajemen sekuriti atau manajemen keamanan adalah langkah-langkah yang perlu diselenggarakan dalam membuat upaya keamanan dan pencegahan kerugian agar tidak terjadi gangguan yang dapat menimbulkan kerugian, dengan dasar efektif dan efisien. Secara umum manusia sebagai individu pada dasarnya mempunyai hasrat yang primer dalam kehidupannya, yaitu hasrat untuk mendapatkan pangan dan hasrat untuk keamanan diri atau mempertahankan diri demi kelangsungan hidupnya menurut (Iskandar & Nurlaila, 2021). Manajemen Sekuriti adalah rangkaian proses kegiatan sekuriti yang dimulai dari perencanaan, pengorganisasian, pelaksanaan serta pengawasan dan pengendalian yang secara professional dan terntegrasi untuk mencegah dan mengurangi kerugian akibat ancaman (Peraturan Kapolri Nomor 24 tahun 2000).

Dalam Pasal 1 Peraturan Kepala Kepolisian Negara Republik Indonesia No. 24 Tahun 2007 mengatakan bahwa Manajemen Sekuriti didefinisikan sebagai bagian dari manajemen secara keseluruhan yang meliputi struktur organisasi, perencanaan, tanggung jawab, pelaksanaan, prosedur, proses, dan sumber daya yang dibutuhkan dalam rangka pengamanan dan pengendalian resiko.

### **Hipotesis**

Hipotesis adalah suatu anggapan teoritis yang dapat dipertegas. Berdasarkan kerangka berpikir diatas, maka dapat dirumuskan suatu hipotesis yang menyatakan bahwa terdapat pengaruh yang signifikan antara Objek Vital, Pengamanan File dan Pengamanan *Cyber* pada PT. Pertamina (Persero) terhadap Manajemen Sekuriti pada PT. Pertamina (Persero).

H<sub>0</sub>: Adanya pengaruh antara Objek Vital, Pengamanan File dan Pengamanan *Cyber* terhadap tingkat keamanan pada PT. Pertamina (Persero).

H<sub>1</sub>: Tidak adanya pengaruh antara Objek Vital, Pengamanan File dan Pengamanan *Cyber* terhadap tingkat keamanan pada PT. PT. Pertamina (Persero)

## **METODOLOGI PENELITIAN**

### **Desain Penelitian**

Subjek dari desain penelitian ini adalah PT. Pertamina (Persero). Adapun analisis data penelitian ini menggugurkan analisis kualitatif dengan pendekatan tinjauan sistematik (*systematic review*). Pendekatan *systematic review* berfungsi untuk merangkum hasil penelitian yang bersifat deksriptif kualitatif. Dalam penelitian ini, pengumpulan data dilakukan melalui *literature review* yang telah membahas tentang Objek Vital, Pengamanan File dan Pengamanan *Cyber* yang terdapat pada PT. Pertamina (Persero).

### **Analisis Data**

Jenis Penelitian ini adalah penelitian kualitatif dengan pendekatan *Systematic Review*. Menurut (Bogdan dan Taylor, 1993) dalam (Prastowo, 2011, p. 22) Metodologi penelitian kualitatif adalah prosedur penelitian yang menghasilkan data diskriptif kualitatif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati. Menurut keduanya pendekatan ini diarahkan pada latar dan individu secara menyeluruh (holistik). Dengan pendekatan ini diharapkan temuan-temuan empiris dapat didiskripsikan secara lebih rinci. Jenis data penelitian adalah berupa fakta empirik yang dikumpulkan peneliti untuk kepentingan pemecahan masalah atau menjawab pertanyaan penelitian. Data penelitian dapat berasal dari berbagai sumber, dikumpulkan menggunakan berbagai teknik selama proses penelitian berlangsung. Sumber data yang digunakan pada penelitian ini adalah data sekunder yaitu data yang diperoleh atau dikumpulkan peneliti dari berbagai sumber yang telah ada. Data sekunder dapat berupa data dari Annual Report PT. Pertamina (Persero) dan sebagainya.

### **Tahapan Penelitian**

Tahapan penelitian adalah tingkatan dalam penelitian yang dilakukan secara terstruktur ataupun sistematis. Dimana banyak manfaat yang akan didapatkan ketika peneliti menyusun tahapan penelitian tersebut, yakni:

1. Pendahuluan. Bab ini membahas secara singkat mengenai latar belakang penelitian, rumusan masalah, tujuan penelitian, kegunaan penelitian yang bila mana penulis peroleh dari penelitian yang dilakukan.
2. Landasan Teori. Bab ini telah menjelaskan landasan teori untuk menjelaskan objek vital, pengelolaan objek vital di PT. Pertamina, pengamanan file, pengamanan file di PT. Pertamina, pengamanan *cyber*, serta pengamanan *cyber* di PT. Pertamina, manajemen keamanan dan hipotesis
3. Metodologi Penelitian. Bab ini berisi tentang desain penelitian, analisis data, tahapan penelitian, tempat dan waktu
4. Pembahasan. Bab ini membahas profil perusahaan di PT. Pertamina keamanan file di PT. Pertamina, dan keamanan *cyber* di PT. Pertamina.
5. Kesimpulan. Bab ini menyajikan kesimpulan asal pembahasan dan saran buat penelitian yang dilakukan.

## **Lokasi dan Waktu**

### **Lokasi Penelitian**

Lokasi dalam penelitian ini dilakukan disalah satu anak Perusahaan PT. Pertamina (Persero), yakni Depo Pertamina Plumpang yang terletak di Jl. Inspeksi Kali Sunter No. Kav 45-46, Kelapa Gading, Kota Jakarta Utara, RT 01/04, Sungai Bambu, Kec. Tanjung Priok, Jakarta Utara, Daerah Khusus Ibukota Jakarta 14330.

### **Waktu Penelitian**

Penelitian ini dilaksanakan dalam waktu 1 bulan yang dimulai dari 1 Mei 2023 hingga 31 Mei 2023.

## **HASIL DAN PEMBAHASAN**

### **Profil Perusahaan**

PT. Pertamina (Persero) adalah Badan Usaha Milik Negara (BUMN) yang telah membangun Indonesia lebih dari 6 dekade melalui penyediaan energi berkelanjutan secara merata. Dalam menjalankan bisnis sebagai perusahaan energi nasional yang terintegrasi di Indonesia. PT. Pertamina (Persero) terbagi ke dalam 6 Subholding dari Hulu ke Hilir yang siap bergerak untuk mencapai target sebagai *Global Energy Champion* dengan nilai pasar US\$ 100 miliar. PT. Pertamina (Persero) juga kembali mencatatkan namanya sebagai satu-satunya perusahaan Indonesia yang masuk dalam daftar Fortune Global 500. Untuk menjalankan bisnis utamanya, perusahaan ini memiliki 6 Subholding yang masing-masing bergerak dibidang hulu, kilang & petrokimia, komersial & perdagangan, gas, listrik & energi terbarukan dan perkapalan. Selain itu, melalui anak-anak usahanya yang lain, perusahaan ini juga berbasis dibidang asuransi, pelayanan kesehatan, penerbangan, dan pengembangan properti.

### **Mengelola Objek Vital Nasional PT. Pertamina (Persero) Terhadap Manajemen Sekuriti**

PT. Pertamina (Persero) untuk memastikan bahwa pemenuhan kebutuhan BBM dan LPG serta memberikan pelayanan kepada masyarakat tetap menjadi prioritas utama Perusahaan. Berdasarkan Keputusan Presiden (Keppres) No. 63 Tahun 2004, infrastruktur energi di wilayah operasi Pertamina merupakan Objek Vital Nasional (Obvitnas) yang harus bebas dari ancaman dan gangguan. Penanganan Objek Vital kegiatan Pertamina di dalam area, yang dilaksanakan oleh petugas keamanan (*security*) atau manajemen sekuriti dan anggota Ditpamobvit Polda, dalam hal mengamankan aset-aset penting, fasilitas maupun dokumen. Sebagai pengamanan langsung Ditpamobvit atau (Direktorat Pengamanan Objek Vital) Polda melaksanakan pengamanan di PT. Pertamina (Persero) Terminal BBM dengan menempatkan anggota sebanyak 5 Personil masing-masing 3 personil pengamanan melekat dan 2 personil sebagai unsur pimpinan (perwira pengendali dilapangan). Pengamanan utama berada pada petugas keamanan (*security*) atau manajemen sekuriti dengan melaksanakan tugas sesuai dengan SOP (*Standar Operasional Prosedure*) dengan tetap berkoordinasi dengan anggota Ditpamobvit Polda yang melaksanakan *Back-up* pengamanan. Pertanggung jawaban keamanan berada di Operation Head (OH) dalam pelaksanaan tugasnya dikendalikan oleh *Chief Security*. Dari kriteria yang terkandung di dalam Keputusan Presiden Nomor 63 Tahun 2004 yang secara normatif disebutkan bahwa pelaksana utama yaitu pengamanan Obvitnas ataupun otoritas pengelola Obvitnas, namun dalam hal *back-up* ialahh pengamanan Polri itu sendiri atau Direktorat Pengamanan Objek Vital (Ditpamobvit).

## **Pengamanan File PT. Pertamina (Persero) Terhadap Manajemen Sekuriti**

PT. Pertamina (Persero) diwajibkan melindungi data para pelanggannya. Setiap data pribadi pelanggan PT. Pertamina pada aplikasi *mobile* yang telah terkumpul di situs MyPertamina diperuntukkan untuk memudahkan PT. Pertamina (Persero) dalam mendata para pelanggan. Aplikasi MyPertamina juga dipertanyakan keamanannya oleh masyarakat, dan sejumlah pengendara menilai aplikasi MyPertamina tidak sejalan dengan larangan penggunaan handphone di dalam SPBU. Seorang pengendara dijumpai di salah satu SPBU. Karena pernah terjadi kebocoran data dari MyPertamina itu sendiri sehingga perusahaan perlu memeriksa terlebih dahulu sistem informasi dari aplikasi MyPertamina yang datanya dibocorkan oleh Bjorka. Jika ditemukan celah atau kebocoran data pada sistem keamanan file, berarti kemungkinan memang terjadi peretasan dan pencurian data yang dilakukan oleh seorang oknum.

## **Pengamanan Cyber pada PT. Pertamina (Persero) Terhadap Manajemen Sekuriti**

Badan Siber dan Sandi Negara (BSSN) melalui Balai Sertifikat Elektronik (BSrE) melakukan penandatanganan Perjanjian Kerjasama dengan PT. Pertamina (Persero). Kerjasama ini merupakan lanjutan dari *Memorandum of Understanding (MoU)* antara BSSN dengan PT. Pertamina (Persero) yang tertuang dalam penandatanganan Perjanjian Kerjasama VP IT Architecture, Security dan Policy PT. Pertamina (Persero). Di era digital seperti saat ini, Pertamina menyadari tantangan, potensi, dan risiko perkembangan dan pemanfaatan teknologi informasi/komunikasi. Selain itu, VP IT Architecture, Security dan Policy sendiri sudah mempunyai inisiatif untuk membuat Pertamina *Cyber Security Incident Implementation* yaitu implementasi untuk meningkatkan ketahanan *cyber* di lingkungan PT. Pertamina (Persero).

PT. Pertamina (Persero) terus meningkatkan standar keamanan dan keselamatan operasional dengan mempercepat penetapan Daerah Terbatas dan Terlarang (DTT). Dalam melaksanakan Kegiatan *sharing session tim Cyber Security Center* Pertamina bekerja sama dengan salah satu perusahaan konsultan IT global yang memiliki kompetensi di bidang *cyber security* dan komunikasi sebagai narasumber. Kegiatan ini untuk memberikan wawasan kepada rekan-rekan *Corporate Secretary* PT. Pertamina *group* sebagai bekal dalam menyikapi situasi krisis dan bagaimana *handling communication*, terutama yang berkaitan dengan *cyber security issue*.

## **Contoh Kasus Pencurian Data pada PT. Pertamina (Persero) oleh Bjorka**

PT. Pertamina pernah mengalami pencurian data pada saat desas-desus BBM naik pada September 2022 lalu, Bjorka menyatakan akan mempublikasi data yang terdapat di aplikasi MyPertamina. Publikasi tersebut untuk mendukung rakyat Indonesia yang tengah berdemo menolak kebijakan pemerintah menaikkan harga BBM. Dua bulan berselang Bjorka membuktikan ancamannya, sebanyak 44.237.264 data dari aplikasi MyPertamina milik PT. Pertamina (Persero) diduga dibocorkan. Dalam unggahan terbarunya bertajuk 'MyPertamina Indonesia 44 Million' disitus *BreachForums*. Bjorka mengaku telah menjual jutaan data tersebut senilai Rp 392 juta dalam bentuk BitCoin. Dalam unggahan Bjorka, tercatat data yang ia curi terdiri atas 30 GB tak terkompresi dan 6 GB terkompresi. Pembocoran data dilakukan pada November ini dengan format CSV (*Comma Separated Value*).

## **PT. Pertamina (Persero) dalam Mengatasi Pengamanan *Cyber* pada Aplikasi MyPertamina**

PT. Pertamina telah menghadapi masalah dengan keamanan aplikasi MyPertamina karena telah dihack beberapa kali oleh seorang peretas bernama Bjorka. PT. Pertamina telah mengambil beberapa tindakan untuk mengamankan aplikasi tersebut. Berikut ini ialah beberapa langkah-langkah yang telah diterapkan oleh PT. Pertamina (Persero) dalam melakukan pengamanan *cyber* pada aplikasi MyPertamina, yaitu:

1. Menanggapi ancaman  
PT. Pertamina (Persero) telah mengeluarkan pernyataan dan mengambil langkah-langkah untuk memastikan keamanan aplikasi sebagai tanggapan atas ancaman hacking.
2. Investigasi Pelanggaran  
PT. Pertamina (Persero) menyelidiki pelanggaran dan menemukan berapa banyak pengguna yang terpengaruh.
3. Transformasi Digital  
PT. Pertamina (Persero) telah memperbaiki infrastruktur digitalnya untuk memberikan layanan yang lebih baik, seperti dengan meluncurkan aplikasi MyPertamina.
4. Layanan Pelanggan Digital  
PT. Pertamina meluncurkan layanan pelanggan digital untuk meningkatkan layanan pelanggan di era digital.

## **KESIMPULAN DAN SARAN**

### **Kesimpulan**

Berdasarkan uraian diatas, maka dapat diambil kesimpulan bahwa adanya pengaruh antara Objek Vital, Pengamanan File dan Pengamanan *cyber* terhadap Manajemen Sekuriti di PT. Pertamina (Persero). Artikel ini ingin mangulas keterkaitannya mengenai Objek Vital dalam mempertahankan operasional PT. Pertamina (Persero), keterkaitannya antara Pengamanan File dan Pengamanan *cyber* dengan Manajemen Sekuriti PT. Pertamina (Persero). PT. Pertamina harus menyusun strategi agar dapat memitigasi resiko keamanan serta melindungi informasi dan sistem data industri. Objek Vital, Pengamanan File dan Pengamanan *cyber*; terhadap PT. Pertamina (Persero) sangatlah penting dalam menjaga keberlanjutan operasional dan keamanan Perusahaan. Kebijakan keamanan yang efektif, tindakan pengamanan *cyber* yang kuat, dan perlindungan yang baik terhadap file dan data akan membantu melindungi PT. Pertamina dari ancaman eksternal yang dapat berpotensi merugikan perusahaan dan pelanggan PT. Pertamina sendiri. PT. Pertamina (Persero) dapat membangun kepercayaan yang lebih besar di kalangan pemangku kepentingan dalam menghadapi tantangan keamanan yang mungkin muncul di masa depan. Penulis berharap artukel ini dapat bermanfaat untuk Perusahaan PT. Pertamina sebagai bahan evaluasi untuk kedepannya, dalam meningkatkan keamanan file ataupun *cyber* yang dapat terjadi sewaktu-waktu dalam dunia digital seperti saat ini.

## DAFTAR PUSTAKA

- Dwipayani. (2022). Kerangka Konsep. <http://repository.poltekkes-denpasar.ac.id/9010/4/BAB%20III%20Kerangka%20Konsep.pdf>
- Gusleni, Y. (2010). Penentuan Prioritas Pelayanan Pengguna Jasa Kereta Api dalam Transportasi Antarmoda di Stasiun Gambir. *Badan Litbang Perhubungan Kementerian Perhubungan*, 22(5), hal. 569–578. <http://ojs.balitbanghub.dephub.go.id/index.php/warlit/article/download/1122/818>
- Hidayat, T. Manajemen Industrial Sekuriti. *Academia*. Retrieved June 7, 2023, from [https://www.academia.edu/19735377/manajemen\\_industrial\\_sekuriti](https://www.academia.edu/19735377/manajemen_industrial_sekuriti)
- Institut Teknologi Sepuluh Nopember. (2023). Keamanan Siber. <https://www.its.ac.id/it/id/keamanan-siber/>
- Iskandar, O., & Nurlaila, S. (2021). Mata Kuliah Manajemen Sekuriti Edisi ke-1 (Vol. 1). <http://repository.ubharajaya.ac.id/16849/1/BAHAN%20ANJAR%20MANAJEMEN%20SEKURIRI%20-%20OKTO%20ISKANDAR%20%26%20BU%20SILVIA%20%20%281%29.pdf>
- Keputusan Presiden RI No. 63 Tahun 2004. Presiden Republik Indonesia. Retrieved May 31, 2023, from [https://jdih.esdm.go.id/peraturan/Keppres No. 63 Thn 2004.pdf](https://jdih.esdm.go.id/peraturan/Keppres%20No.%2063%20Thn%202004.pdf)
- Namudat, H., Karlina, N., & Rusli, B. (2018). Analisis Kebijakan Pengamanan Objek Vital di PT. FREEPORT Indonesia. *Jurnal Pemikiran Dan Penelitian Bidang Administrasi, Sosial, Humaniora Dan Kebijakan Publik*, 1(2), hal. 39–44. <https://doi.org/10.24198/responsive.v1i2.20673>
- Pertamina. (2020). Keamanan Siber Perusahaan. <https://www.pertamina.com/id/keamanan-siber-perusahaan>
- Pertamina. (2020). Kelola Objek Vital Nasional, Pertamina Prioritaskan Pelayanan BBM dan LPG Untuk Rakyat. <https://www.pertamina.com/id/news-room/news-release/kelola-objek-vital-nasional-pertamina-prioritaskan-pelayanan-bbm-dan-lpg-untuk-rakyat>
- Prastowo. (2011). Penerapan SMK3 di CV Roda Jati. <http://e-journal.uajy.ac.id/11821/4/TI069043.pdf>
- Pratama, A. S. (2019). Analisis Risiko K3 Menggunakan Pendekatan HIRADC dan JSA (Studi Kasus: Proyek Pembangunan Sistem Pengamanan Kilang Terpadu Tahap II PT. Pertamina RU VI Balongan). [https://www.academia.edu/download/63082308/Laporan\\_Kerja\\_Praktik\\_Analisis\\_Risiko\\_K3\\_Menggunakan\\_Pendekatan\\_HIRADC\\_dan\\_JSA\\_oleh\\_Akhmad\\_Setyawan\\_Pratama\\_201920200424-123232-1w1yy0r.pdf](https://www.academia.edu/download/63082308/Laporan_Kerja_Praktik_Analisis_Risiko_K3_Menggunakan_Pendekatan_HIRADC_dan_JSA_oleh_Akhmad_Setyawan_Pratama_201920200424-123232-1w1yy0r.pdf)
- Soesanto, E., Purba, L. M., Aprilia, B., Putra, D. R., & Putri, S. D. (2023). Implementasi Objek Vital, Pengamanan File dan Pengamanan Cyber di PT. Pertamina. *IJM: Indonesian Journal of Multidisciplinary*, 1(1), hal. 96–105. <https://journal.csspublishing.com/index.php/ijm/article/view/92>
- Suheri, A. (2017). Keamanan File dengan Teknik Zigzag dan Huffman. *Media Jurnal Informatika*, 9(2), hal. 78–83. <https://doi.org/10.35194/mji.v9i2.450>
- Winarto, W. W. A. (2021). Analisis Review Penggunaan Sistem Informasi pada PT. Pertamina. *BIOS: Jurnal Teknologi Informasi Dan Rekayasa Komputer*, 2(2), hal. 51–59. <https://doi.org/10.37148/bios.v2i2.20>