Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen
E-ISSN: 2829-7547 | Vol. 02, No. 06, 2024, pp. 196-212
https://journal.uii.ac.id/selma/index

OPEN ACCESS

Artikel Hasil Penelitian

Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede

Fikri Irfan Adristi[a)], Erika Ramadhani

Department of Informatics, Faculty of Industrial Technology
Universitas Islam Indonesia, Sleman, Special Region of Yogyakarta
Indonesia

[a)]Corresponding author: fikri.adristi@students.uii.ac.id

ABSTRAK

Insiden kebocoran data di Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya menunjukkan pentingnya penerapan budaya keamanan siber yang efektif dalam sebuah organisasi. Penelitian ini bertujuan untuk menganalisis dampak kebocoran data PDNS 2 Surabaya melalui pendekatan Matriks Budaya Keamanan Siber yang dan Matriks Dimensi Budaya Nasional Hofstede dengan data sampel berita yang diperoleh secara *online*. Tanggal publikasi beritanya adalah 26 Juni 2024 - 10 Juli 2024. Keterbatasan penelitian ini terletak pada sumber data yang hanya berasal dari berita *online*. Implikasi manajerial diberikan dari aspek manajemen puncak dan karyawan. Kesimpulan penelitian ini diuraikan dari aspek: (1) Kebutuhan akan peningkatan kesadaran dan pendidikan keamanan; (2) pentingnya penerapan dan kepatuhan terhadap kebijakan keamanan; (3) respons cepat dan efektif terhadap insiden; (4) pengembangan proses pemulihan dan backup data yang kuat; (5) orientasi jangka panjang dalam pengelolaan keamanan informasi; serta (6) penegakan disiplin dan pengendalian internal.

Kata Kunci: kebocoran data, PDNS 2 Surabaya, budaya keamanan siber, dimensi budaya nasional Hofstede, keamanan informasi

PENDAHULUAN

Dalam era digital yang semakin maju, keamanan siber menjadi perhatian utama bagi organisasi di seluruh dunia. Kebocoran data yang terjadi di Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya menggambarkan betapa pentingnya penerapan budaya keamanan siber yang efektif dalam sebuah organisasi. PDNS 2 di Surabaya mengalami serangan siber dalam bentuk *ransomware* bernama *Brain Chiper*, varian terbaru dari Lockbit 3.0. Puncaknya, PDNS mulai tidak bisa diakses sejak Kamis (20/6) yang berakibat layanan publik tidak bisa diakses, termasuk layanan imigrasi (Rochman, 2024). Fenomena kebocoran data ini tidak hanya berdampak pada kerugian finansial, tetapi juga menurunkan kepercayaan publik dan membahayakan informasi sensitif.

Seperti disarikan pemangku kepentingan atas pusat data nasional (PDN) bisa melakukan penuntutan kepada pengelola PNDS 2 Surabaya karena lalai dalam tata kelola. Permintaan maaf dinilai tidaklah cukup. Alfons Tanujaya, praktisi keamanan siber dari Vaksincom menekankan pentingnya konsistensi dalam standarisasi kualitas layanan yang tercermin dalam *Service Level Agreement* (SLA), yang menegaskan adanya pertanggungjawaban termasuk secara finansial atas kelalaian pengelola jasa *cloud* jika terjadi gangguan atau peretasan. "Lembaga lain yang menggunakan layanan ini, jika datanya hilang, mereka berhak menuntut," ujarnya. Ditjen Imigrasi Kemenkumham atau institusi negara lainnya bisa menagih hak yang tidak dipenuhi pengelola (Bloomberg Technoz, 2024; Puspitasari, 2024).

TelkomSigma, anak usaha PT Telkom, ditunjuk Kementerian Kominfo untuk mengelola pusat data sementara. Data ditempatkan di Surabaya sesuai amanat Perpres Sistem Pemerintah Berbasis Elektronik (SPBE), khususnya Pasal 27. Alfons menegaskan bahwa Telkom selaku *vendor* pusat data seharusnya memikul beban tanggung jawab terbesar atas insiden peretasan PDNS 2 Surabaya (Bloomberg Technoz, 2024; Puspitasari, 2024). Kejadian ini turut menyebabkan Semuel Abrijani Pangerapan mengundurkan diri dari kursi Direktur Jenderal Aplikasi dan Informatika (Aptika) Kominfo usai insiden peretasan PDNS 2. Ia menyebut pengunduran dirinya merupakan tanggung jawab moral atas insiden tersebut (CNN Indonesia, 2024c; Rochman, 2024).

Jika ditinjau dari sudut pandang sisi budaya keamanan dalam organisasi, seharusnya organisasi harus mempunyai prosedur respons cepat atas serangan siber berupa *incident response plan* (RCP), *disaster recovery plan* (DRP), dan *business continuity plan* (BCP) (EC-Council, 2022). Namun, beberapa penelitian sejenis sebelumnya seperti (AlHogail, 2015; Tsoeu dan da Veiga, 2022; Mikuletič *et al.*, 2024; Niemimaa, 2024; Tenzin, McGill dan Dixon, 2024) relatif terbatas memperhatikan bagaimana dimensi budaya organisasi, seperti yang dijelaskan oleh Dimensi Budaya Nasional Hofstede, mempengaruhi implementasi dan efektivitas dari prosedur-prosedur ini. Salah satu kerangka kerja yang dapat digunakan untuk memahami budaya organisasi adalah Dimensi Budaya Nasional Hofstede.

Penelitian ini bertujuan untuk mengisi *gap* tersebut dengan menganalisis dampak kebocoran data PDNS 2 Surabaya melalui pendekatan Matriks Budaya Keamanan Siber yang dan Matriks Dimensi Budaya Nasional Hofstede dengan data sampel berita yang diperoleh secara *online*. Dengan menggabungkan kedua pendekatan ini, diharapkan dapat diperoleh pemahaman yang lebih komprehensif mengenai faktor-faktor budaya yang mempengaruhi efektivitas keamanan siber dalam organisasi.

KAJIAN LITERATUR

Budaya Keamanan Siber

Menurut Alvarez-Dionisi dan Urrego-Baquero (2019) budaya keamanan siber adalah "pengetahuan, keyakinan, persepsi, sikap, asumsi, norma, dan nilai masyarakat mengenai keamanan siber dan bagaimana hal tersebut terwujud dalam perilaku masyarakat terhadap teknologi informasi." Pada kenyataannya, tujuan utama budaya keamanan siber adalah untuk mengembangkan dan menerapkan ekosistem budaya keamanan siber untuk mendukung keamanan siber. Berbagi pengalaman dalam membangun landasan sosial dan psikologis yang canggih dapat membantu mendukung keamanan siber .

Budaya Keamanan Siber mencakup topik-topik umum termasuk kesadaran keamanan siber dan kerangka kerja keamanan informasi, namun cakupan dan penerapannya lebih luas, karena berkaitan dengan menjadikan pertimbangan keamanan informasi sebagai

bagian integral dari pekerjaan, kebiasaan, dan perilaku karyawan, serta menanamkannya dalam keseharian mereka. tindakan" (Oltsik, 2024).

Menurut Harper (2023) guna membangun budaya keamanan siber yang efektif, sebuah organisasi harus mengetahui masalah utama yang mereka hadapi. Meskipun ancaman dunia maya berubah setiap hari dan bahkan dalam hitungan menit, ada beberapa aspek inti yang dapat menjadi fokus organisasi untuk membangun budayanya. Ada lima masalah sulit, skalabilitas dan komposisi, kebijakan, metrik keamanan, ketahanan, dan perilaku manusia.

Dimensi Budaya Nasional Hofstede

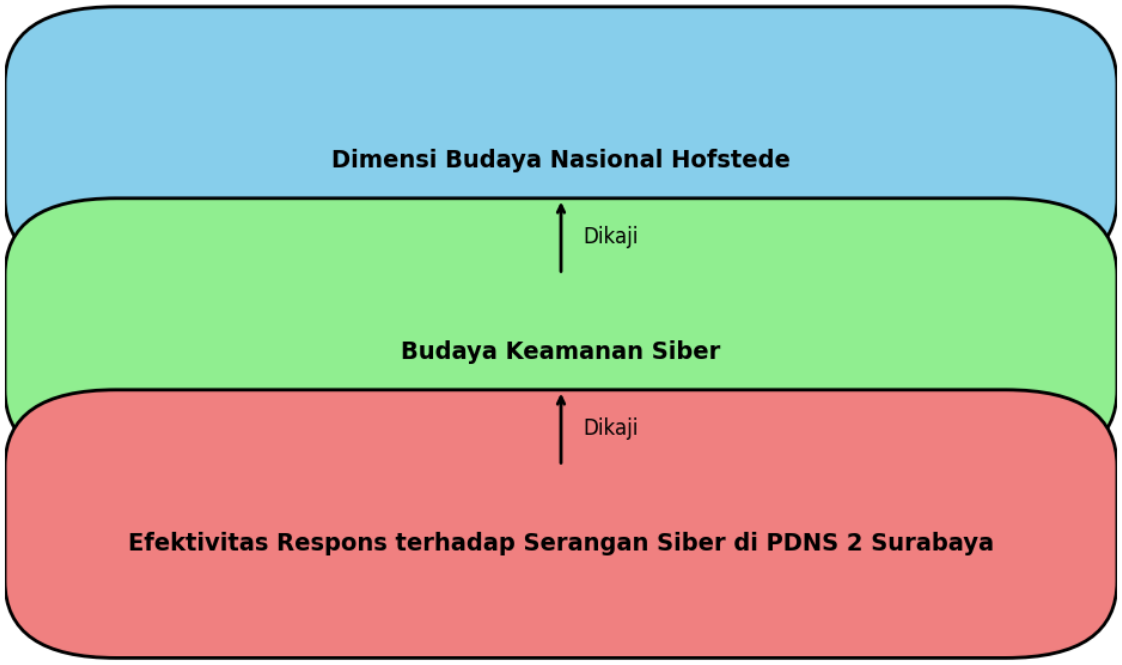
Menurut Wardani dan Nurainun'nisa (2024) Budaya Hofstede adalah program mental yang mempengaruhi cara orang berpikir dan bertindak. Program mental ini, ketika dimiliki oleh sekelompok orang dalam suatu negara, secara kolektif disebut sebagai budaya nasional. Budaya Hofstede memiliki 5 (lima) dimensi yang terdiri dari *power distance; individualism versus collectivism; masculinity versus feminism; uncertainty avoidance;* dan *long term orientation versus short term orientation* dengan penjabarannya sebagai berikut (Pratiwi, 2017; Sari dan Dirgahayu, 2017; Molle *et al.*, 2024):

1. Dimensi pertama budaya hofstede yang ada di indonesia ini yaitu dimensi *power distance*. Dimensi *power distance* ini didefinisikan sebagai sejauhmana anggota institusi dan organisasi yang kurang kuat disuatu negara tersebut mengharapkan dan menerima bahwa kekuasaan tersebut didistribusikan secara tidak adil. Dimensi ini menerangkan bagaimana sikap pegawai pemerintah yang tidak memiliki jabatan/kekuasaan dalam suatu instansi terhadap pegawai yang memiliki jabatan/kekuasaan.
2. Dimensi kedua adalah dimensi *collectivism versus individualism* yang merupakan dimensi perbedaan antara pegawai *individualism* dan pegawai *collectivism*. Pegawai yang *individualism* adalah pegawai yang lebih menjaga dirinya sendiri dan tidak suka berkelompok, sedangkan pegawai yang *collectivism* adalah pegawai yang lebih menjaga kelompoknya daripada dirinya sendiri.
3. Dimensi budaya hofstede yang ketiga yaitu *masculine versus feminism*. *Masculine* merupakan suatu dimensi yang dapat memotivasi orang agar menjadi yang terbaik. Dimensi *masculine* yang memiliki nilai tinggi ditunjukkan oleh pegawai yang terdorong akan adanya pencapaian dalam berprestasi, persaingan dan kesuksesan di tempat kerja atau suatu instansi pemerintah, sedangkan *feminism* ditekankan bahwa nilai-nilai kehidupan lebih didominasi oleh kualitas hidup, kepedulian sesama, pelayanan. *Feminism* memotivasi pegawai untuk bekerja dengan menanamkan nilai-nilai yang lembut untuk menciptakan hubungan baik antara pegawai atau masyarakat dengan bekerja sama agar mencapai keamanan dan kenyamanan.
4. *Uncertainty Avoidance* merupakan dimensi budaya Hofstede Keempat yang berkaitan dengan cara pegawai dalam menghadapi fakta tentang masa depan yang tidak diketahui. Dimensi ini dapat dilihat dengan tindakan pegawai yang merasa terancam oleh situasi beresiko dan tidak pasti sehingga mereka berusaha meminimalkan resiko dengan mengembangkan hukum atau peraturan formal dalam suatu instansi pemerintah.
5. Dimensi budaya Hofstede yang Kelima yaitu *long term orientation versus short term orientation*. *Long term orientation* adalah dimensi budaya di mana individu memikirkan akibat jangka panjang yang akan terjadi ketika mereka melakukan suatu tindakan di masa sekarang, sedangkan *short term orientation* adalah dimana individu lebih fokus pada masa lalu dan masa kini

Information Security Awareness

Information security awareness (ISA) mengacu pada kondisi kesadaran dimana *user* secara ideal berkomitmen pada aturan, mengenali potensi, memahami pentingnya tanggung jawab, dan bertindak sesuai dengan itu. Meskipun banyaknya kasus pelanggaran keamanan informasi, khususnya pada *knowledge-based institution*, yang diakibatkan oleh keengganan pengguna untuk mematuhi pedoman keamanan dan tindakan efektif seperti penerapan *incident response plan* (RCP), *disaster recovery plan* (DRP), dan *business continuity plan* (BCP) yang harus dilakukan untuk mengantisipasi dampak negatifnya (Ahlan, Lubis dan Lubis, 2015).

Menurut Ashraf (2005) *information security awareness* adalah pendidikan dan kesadaran pengguna untuk menangani ancaman keamanan informasi dan meminimalkan dampaknya. Program kesadaran pada dasarnya memusatkan perhatian pada masalah keamanan informasi seperti *confidentiality, integrity, and availability*. Ini menyoroti pentingnya faktor-faktor ini, perannya dalam bisnis dan akhirnya berkonsentrasi pada bagaimana berperilaku dengan faktor-faktor tersebut dengan cara yang percaya diri.



Gambar 1. Analisis Dampak Kebocoran Data PDNS 2 Surabaya

METODE

Penelitian ini merupakan penelitian berjenis penelitian kualitatif. Penelitian ini merupakan penelitian kualitatif dengan pendekatan deskriptif. Menurut Merriam (2009) penelitian kualitatif berfokus pada makna dalam konteks, sehingga memerlukan instrumen pengumpulan data yang peka terhadap makna yang mendasarinya ketika mengumpulkan dan menafsirkan data. Data sampel yang digunakan merupakan data yang bersumber dari berita *online* yang mana spesifikasi datanya terdapat pada tabel 1 dibawah. Pendekatan analisis data

pada penelitian ini adalah pendekatan pemetaan dan matriks seperti pada penelitian (Kwon *et al.*, 2020).

Tabel 1. Spesifikasi Data

Spesifikasi	Deskripsi
Sumber Data	Berita *online* dari berbagai sumber (Anggraeni, 2024b, 2024a; CNN Indonesia, 2024b, 2024a; Fadilah, 2024; Hadyan, 2024; Kure, 2024; Rahmawati, 2024; Safitri, 2024; Wakang, 2024).
Jenis Data	Penilaian budaya keamanan siber dan dimensi budaya Hofstede
Kategori Penilaian	Kebijakan, pelatihan, insiden, kepatuhan, sikap pengguna, dimensi budaya (*Individualism, Power Distance,* dll.)
Rentang Waktu	Tanggal publikasi sampel berita (26 Juni 2024 - 10 Juli 2024)
Frekuensi	Jumlah berita yang dianalisis per bulan
Format Data	Teks deskriptif dan skor numerik
Metodologi	Analisis konten berita terkait budaya keamanan siber dan dimensi budaya Hofstede serta penilaian dari berita.

HASIL DAN PEMBAHASAN

Kronologi Serangan Siber PDNS 2 Surabaya

Berdasarkan informasi yang dihimpun dari (Aranditio, 2024; Luthfiani, 2024) maka kronologi serangan siber PDNS 2 Surabaya tersaji pada tabel 2 dibawah ini:

Tabel 2. Kronologi Serangan Siber PDNS 2 Surabaya

Tanggal dan Waktu	Uraian Peristiwa
Kamis, 20 Juni 2024 Pukul 00.54 WIB	Terjadi gangguan pada PDNS berupa instalasi *filemalicious* yang menghapus sistem file penting dan menonaktifkan layanan yang sedang berjalan.
Kamis, 20 Juni 2024 Pukul 00.55 WIB	Windows Defender mengalami *crash* dan tidak bisa beroperasi.
Kamis, 20 Juni 2024 Pukul 04.00 WIB	Instansi pertama yang melaporkan dampak gangguan adalah Direktorat Jenderal Imigrasi Kementerian Hukum dan HAM mengenai layanan keimigrasian.
Kamis, 20 Juni 2024 Sore	Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika Semuel Abrijani Pangerapan membenarkan adanya gangguan pada Pusat Data Nasional yang berdampak pada sejumlah layanan publik.
Minggu, 23 Juni 2024	Badan Siber dan Sandi Negara (BSSN) menyatakan tengah melakukan analisis berdasarkan bukti digital masih terus dilakukan, tetapi akar masalah belum juga ditemukan.

Tanggal dan Waktu	Uraian Peristiwa
Senin, 24 Juni 2024	Kepala BSSN mengatakan gangguan PDNS disebabkan oleh serangan siber perangkat keras perusak atau *ransomware brain chipper*, varian dari *ransomware Lockbit 3.0*. Pelaku peretasan Pusat Data Nasional (PDN) meminta uang sebanyak USD 8 juta atau sekitar Rp 131 miliar dalam kurs Rp 16.399 kepada Pemerintah Indonesia.
Selasa, 25 Juni 2024	Direktur Jenderal Aplikasi Informatika Kementerian Kominfo Semuel Abrijani Pangerapan mengatakan pihaknya masih memulihkan layanan di 282 instansi layanan publik yang menggunakan PDNS.

Sumber: (Aranditio, 2024; Luthfiani, 2024)

Mekanisme *Ransomware Brain Chipper* Bekerja

Berikut dibawah pada tabel 3 dibawah ini disajikan *pseudo code* untuk *ransomware* sederhana yang disebut *"Brain Chipper"*. *Pseudo code* ini akan menjelaskan langkah-langkah umum yang diambil oleh *ransomware* untuk mengenkripsi file dan meminta tebusan.

Tabel 3. *Ransomware Pseudo Code*

Pseudo code ransomware

```
# Inisialisasi
generate_encryption_key()
store_key_on_server()

# Scanning File
for each file in target_directories:
    if file_extension in target_extensions:
        encrypt_file(file)

# Enkripsi File
function encrypt_file(file):
    read file content
    encrypt content with encryption_key
    write encrypted content back to file

# Hapus File Asli (Opsional)
function delete_original_file(file):
    delete file

# Pesan Tebusan
create_ransom_note()
save_ransom_note_in_directories()

# Monitoring Pembayaran
```

Pseudo code ransomware

```
while not payment_received():
    wait()
# Dekripsi File (Jika Pembayaran Diterima)
if payment_received():
    send_decryption_key_to_victim()

# Dekripsi File
function decrypt_file(file, decryption_key):
    read encrypted file content
    decrypt content with decryption_key
    write decrypted content back to file
```

Penjelasan:

1. Inisialisasi: Menghasilkan kunci *enkripsi* dan menyimpannya di server penyerang.
2. *Scanning File*: Mencari file dengan ekstensi tertentu di direktori target.
3. Enkripsi File: Membaca, mengenkripsi, dan menulis ulang konten file.
4. Hapus File Asli: Opsional, dapat dilakukan untuk memastikan file asli hilang.
5. Pesan Tebusan: Membuat dan menyimpan pesan tebusan di komputer korban.
6. Monitoring Pembayaran: Menunggu hingga pembayaran diterima.
7. Dekripsi File: Mengirim kunci dekripsi kepada korban dan mendekripsi file.

Pseudo code ini memberikan gambaran umum tentang cara kerja *ransomware*, tetapi tentu saja ada banyak detail tambahan yang terlibat dalam implementasi nyata. Perlu diingat bahwa *pseudo code* ini hanya untuk tujuan pembelajaran dan tidak boleh digunakan untuk kegiatan berbahaya atau ilegal.

Analisis Matriks Penilaian Budaya Keamanan Siber

Berikut dibawah ini disajikan tabel 4. hasil analisis matriks penilaian budaya keamanan siber. Dengan menggunakan matriks ini, organisasi terkait kebocoran data PDNS 2 Surabaya dapat mengidentifikasi area yang perlu diperbaiki dan mengambil tindakan yang tepat untuk meningkatkan budaya keamanan guna merespons serangan siber dengan lebih efektif.

Tabel 4. Analisis Matriks Penilaian Budaya Keamanan Siber

Kriteria/Indikator	Kesadaran Keamanan	Pelanggaran Kepatuhan	Respons Insiden	*Disaster Recovery Plan* (DRP)	*Business Continuity Plan* (BCP)
Peran Serta Karyawan		Terjadi *Insider Threat* dari Mantan Karyawan (Hadyan, 2024; Kure, 2024).			
Tingkat Pengetahuan Karyawan	Terjadi kelalaian SDM akibat penonaktifkan fitur keamanan Windows				

Kriteria/Indikator	Kesadaran Keamanan	Pelanggaran Kepatuhan	Respons Insiden	*Disaster Recovery Plan* (DRP)	*Business Continuity Plan* (BCP)
	Defender (CNN Indonesia, 2024b).				
Penerapan Kebijakan					Pemerintah bakal menyiapkan 4 lapis pencadangan *(backup)* usai Pusat Data Nasional Sementara (PDNS) 2 diserang *ransomware* (Fadilah, 2024).
Kepatuhan terhadap Standar				PDNS 2 Tidak Punya Data Cadangan *(Backup)* (Anggraeni, 2024a).	Imbas Peretasan PDNS, Pemerintah Godok Aturan Kewajiban *Backup Data* (CNN Indonesia, 2024a).
Audit Internal & Kecepatan Respons			Kepala BSSN Hinsa Siburian menjelaskan bahwa pada tanggal 20 Juni 2024, setelah menerima laporan tentang serangan atau gangguan di Surabaya, pihaknya langsung mengadakan rapat koordinasi dengan *incident response team* pada hari yang sama (Rahmawati, 2024).	Dampak Server PDNS *Down*, BSSN Lakukan Audit Digital Forensik (Anggraeni, 2024b).	BPKP Audit Tata Kelola PDN Buntut Peretasan (Safitri, 2024).

Analisis budaya keamanan informasi dalam tabel 4. analisis matriks penilaian budaya keamanan siber menunjukkan beberapa aspek penting yang dapat dibahas dengan mengaitkan teori dan penelitian terdahulu. Berikut dibawah ini adalah pembahasan naratif yang mengaitkan data dalam tabel 4 dengan teori dan penelitian tentang budaya keamanan informasi.

Kesadaran dan Peran Serta Karyawan

Peran serta karyawan dalam keamanan informasi merupakan faktor kunci dalam membangun budaya keamanan yang kuat. Berdasarkan pada tabel 4. analisis matriks penilaian budaya keamanan siber, terlihat adanya ancaman dari dalam *(insider threat)* yang berasal dari mantan karyawan. Penelitian oleh D'Arcy, Hovav dan Galletta (2009) hasilnya menunjukkan bahwa ada tiga praktik yang mencegah penyalahgunaan *intentional insider misuse of information systems resources* (i.e., *IS misuse*): kesadaran pengguna akan kebijakan keamanan; program *security education, training, and awareness* (SETA); dan pemantauan komputer. Hasilnya juga menunjukkan bahwa sanksi yang dirasakan lebih berat dalam mengurangi penyalahgunaan *IS misuse* dibandingkan kepastian sanksi.

Tingkat Pengetahuan Karyawan

Tingkat pengetahuan karyawan juga merupakan indikator penting dalam budaya keamanan informasi. Berdasarkan pada tabel 4. analisis matriks penilaian budaya keamanan siber, menunjukkan bahwa terjadi kelalaian SDM yang mengakibatkan penonaktifan fitur keamanan Windows Defender. Dukungan dan pelatihan dari organisasi kepada karyawannya tentunya mengarahkan pada perilaku keamanan informasi yang positif. Program kesadaran keamanan informasi pada dasarnya memusatkan perhatian pada masalah keamanan informasi seperti *confidentiality, integrity, and availability* (Ashraf, 2005; Ayanwale *et al.*, 2023; Katsantonis *et al.*, 2023; Saeed, 2023).

Penerapan Kebijakan dan Kepatuhan

Kepatuhan terhadap kebijakan keamanan informasi sangat penting untuk memastikan bahwa prosedur keamanan diikuti dengan konsisten. Berdasarkan pada tabel 4. analisis matriks penilaian budaya keamanan siber, menunjukkan bahwa pemerintah sedang menyiapkan beberapa lapis pencadangan *(backup)* untuk meningkatkan ketahanan terhadap serangan *ransomware*. Alraja, Butt dan Abbod (2023) menemukan bahwa ketakutan dan nilai peran mempunyai pengaruh yang signifikan terhadap niat terhadap ISPC. Dukungan dari organisasi juga penting dalam penerapan kebijakan dan kepatuhan keamanan informasi yang efektif (Alraja, Butt dan Abbod, 2023; Ayanwale *et al.*, 2023; Bhagat dan Pravin, 2023).

Audit Internal dan Kecepatan Respons

Audit internal dan kecepatan respons terhadap insiden keamanan informasi mencerminkan kesiapan organisasi dalam menghadapi ancaman. Berdasarkan pada tabel 4. analisis matriks penilaian budaya keamanan siber, Kepala BSSN Hinsa Siburian langsung mengadakan rapat koordinasi setelah menerima laporan tentang serangan, menunjukkan respons yang cepat (Rahmawati, 2024). Audit internal yang rutin dan respons cepat terhadap insiden adalah bagian penting dari strategi keamanan informasi. Respons yang cepat dapat mengurangi dampak dari insiden dan mempercepat proses pemulihan (EC-Council, 2022; Ali, Al-Khalidi dan Al-Zaidi, 2024).

Disaster Recovery Plan (DRP) dan *Business Continuity Plan* (BCP)

Disaster recovery plan (DRP) dan *business continuity plan* (BCP) adalah komponen penting dalam budaya keamanan informasi. Berdasarkan pada tabel 4. analisis matriks penilaian budaya keamanan siber, menunjukkan bahwa PDNS 2 tidak memiliki data cadangan *(backup)* yang memadai dan pemerintah sedang menggodok aturan kewajiban *backup* data *Disaster recovery plan* (DRP) dan *business continuity plan* (BCP) yang solid dapat membantu organisasi untuk segera pulih dari insiden dan melanjutkan operasi bisnis (EC-Council, 2022).

Dengan mengintegrasikan teori dan penelitian terdahulu, dapat disimpulkan bahwa memperkuat partisipasi karyawan, meningkatkan pengetahuan, memastikan kepatuhan terhadap kebijakan, melakukan audit internal secara rutin, serta memiliki rencana pemulihan yang solid adalah langkah-langkah penting dalam membangun budaya keamanan informasi yang kuat.

Analisis Matriks Penilaian Penilaian Budaya Nasional Hofstede

Berikut dibawah ini disajikan tabel 5. hasil analisis matriks penilaian budaya nasional Hofstede. Dengan menggunakan matriks ini, organisasi terkait kebocoran data PDNS 2 Surabaya dapat mengidentifikasi area yang perlu diperbaiki dan mengambil tindakan yang tepat untuk meningkatkan budaya keamanan guna merespons serangan siber dengan lebih efektif.

Tabel 5. Analisis Matriks Penilaian Budaya Keamanan Siber

Dimensi Hofstede	Penilaian Berdasarkan Kasus PDNS 2	Interpretasi
Power Distance (Jarak Kekuasaan)	Rapat koordinasi langsung dilakukan oleh Kepala BSSN setelah insiden terjadi.	Jarak kekuasaan tinggi terlihat dari keputusan yang diambil oleh otoritas tertinggi (Kepala BSSN) dalam merespons insiden tanpa perlu proses berjenjang.
Individualism vs Collectivism	Partisipasi karyawan dalam keamanan informasi masih kurang dan ada ancaman dari dalam *(insider threat)*.	Budaya kolektivisme kurang kuat, terlihat dari kurangnya partisipasi dan kesadaran karyawan dalam menjaga keamanan informasi bersama.
Masculinity vs Femininity	Penekanan pada tindakan mitigasi dan respons cepat terhadap insiden.	Penekanan pada hasil (maskulinitas) lebih dominan, di mana tindakan cepat dan konkrit diambil untuk mengatasi masalah, menunjukkan orientasi pada pencapaian.
Uncertainty Avoidance (Penghindaran Ketidakpastian)	Pemerintah menyiapkan lapis pencadangan *(backup)* dan peraturan kewajiban *backup* data.	Penghindaran ketidakpastian tinggi, dengan langkah-langkah mitigasi dan aturan baru untuk mencegah insiden serupa di masa depan.
Long-term vs Short-term Orientation	Penekanan pada audit digital forensik dan rencana simulasi rutin respons insiden PDNS	Orientasi jangka panjang terlihat dari investasi dalam audit dan rencana simulasi rutin untuk

Dimensi Hofstede	Penilaian Berdasarkan Kasus PDNS 2	Interpretasi
Indulgence vs Restraint	Tindakan responsif dan kebijakan mitigasi yang tegas.	meningkatkan ketahanan terhadap insiden di masa depan. Budaya pengendalian *(restraint)* terlihat dari kebijakan dan tindakan tegas yang diambil untuk menjaga keamanan dan stabilitas seperti Pemerintah Godok Aturan Kewajiban *Backup* Data.

Analisis budaya nasional Hofstede dalam tabel 5. analisis matriks penilaian budaya nasional Hofstede menunjukkan beberapa aspek penting yang dapat dibahas dengan mengaitkan teori dan penelitian terdahulu. Berikut dibawah ini adalah pembahasan naratif yang mengaitkan data dalam tabel 5 dengan teori dan penelitian tentang budaya nasional Hofstede.

Pembahasan Berdasarkan Dimensi Budaya Nasional Hofstede

Dalam kasus PDNS 2, terlihat bahwa keputusan penting diambil langsung oleh otoritas tertinggi, yakni Kepala BSSN. Hal ini mencerminkan jarak kekuasaan yang tinggi, di mana otoritas pusat memiliki kekuatan besar dalam pengambilan keputusan tanpa melalui proses hierarkis yang panjang. Hofstede, Hofstede dan Minkov (2010) menyatakan bahwa dalam budaya dengan jarak kekuasaan tinggi, keputusan cenderung diambil oleh individu di posisi otoritas tertinggi.

Kurangnya partisipasi karyawan dalam menjaga keamanan informasi dan adanya ancaman dari dalam menunjukkan bahwa budaya kolektivisme masih lemah. Hofstede, Hofstede dan Minkov (2010) mengemukakan bahwa dalam budaya kolektivis, karyawan biasanya memiliki rasa tanggung jawab bersama dan berkolaborasi untuk mencapai tujuan bersama. Ketiadaan ini dapat menjadi faktor penyebab masalah keamanan yang terjadi.

Respons cepat dan tindakan mitigasi yang dilakukan oleh pemerintah menunjukkan orientasi pada hasil dan pencapaian, karakteristik dari budaya maskulin. Hofstede, Hofstede dan Minkov (2010) menjelaskan bahwa dalam budaya maskulin, nilai-nilai seperti keberanian, kompetisi, dan pencapaian hasil sangat diutamakan, seperti yang terlihat dalam penanganan insiden oleh pemerintah.

Langkah-langkah mitigasi seperti pencadangan data *(backup)* dan pembuatan aturan baru menunjukkan tingkat penghindaran ketidakpastian yang tinggi. Hofstede, Hofstede dan Minkov (2010) menunjukkan bahwa dalam budaya dengan penghindaran ketidakpastian yang tinggi, ada keinginan kuat untuk mengontrol masa depan dengan peraturan dan prosedur yang ketat untuk mengurangi risiko ketidakpastian.

Investasi dalam audit digital forensik dan rencana pelatihan simulasi insiden pemulihan yang diinisiasi oleh PPI Dunia menunjukkan orientasi jangka panjang (Wakang, 2024). (Hofstede dan Minkov, 2010; Hofstede, Hofstede dan Minkov, 2010) menekankan bahwa budaya dengan orientasi jangka panjang cenderung fokus pada perencanaan dan investasi untuk masa depan, menunjukkan kesadaran akan pentingnya persiapan untuk tantangan yang mungkin datang.

Tindakan tegas dan kebijakan mitigasi menunjukkan budaya pengendalian *(restraint)*, di mana ada regulasi ketat dan tindakan disiplin untuk menjaga stabilitas dan keamanan.

Hofstede, Hofstede dan Minkov (2010) menyatakan bahwa dalam budaya pengendalian, kebebasan individu dibatasi oleh aturan ketat untuk menjaga keteraturan dan keselamatan bersama.

Dengan menggunakan dimensi budaya nasional Hofstede, kita dapat melihat bagaimana karakteristik budaya mempengaruhi respons dan penanganan insiden keamanan informasi di PDNS 2. Pemahaman ini dapat membantu dalam merancang strategi keamanan yang lebih efektif dan sesuai dengan konteks budaya setempat.

KETERBATASAN PENELITIAN

Keterbatasan penelitian ini terletak pada sumber data yang hanya berasal dari berita *online*. Agar dapat menggali informasi lebih mendalam dan menghasilkan analisis yang lebih komprehensif, diperlukan data hasil wawancara dengan para aktor dan *stakeholders* yang terlibat dalam peristiwa kebocoran data PDNS 2 Surabaya ini.

IMPLIKASI MANAJERIAL

Implikasi manajerial yang dapat diberikan berdasarkan hasil penelitian ini adalah sebagai berikut: Perbaiki bahasanya agar saling nyambung dan naratif:

1. Pelatihan dan Edukasi Keamanan Informasi: Penting untuk melakukan simulasi dan pelatihan keamanan informasi secara berkala guna meningkatkan pengetahuan dan kesadaran karyawan. Manajemen puncak juga perlu dilibatkan dalam sosialisasi dan dukungan pelatihan untuk memastikan partisipasi aktif karyawan yang bekerja di PDNS 2.
2. Penerapan Kebijakan Keamanan yang Ketat: Kebijakan keamanan yang rinci dan jelas perlu ditetapkan dan dipastikan bahwa semua karyawan memahami serta mematuhi kebijakan tersebut. Evaluasi dan audit berkala dari pihak internal dan pihak ketiga perlu dilakukan untuk memastikan kepatuhan terhadap kebijakan keamanan informasi.
3. Peningkatan Proses *Backup* dan Pemulihan Data: Sistem pencadangan data berlapis perlu diimplementasikan untuk meningkatkan ketahanan terhadap serangan siber. Prosedur pemulihan bencana yang komprehensif juga harus disiapkan dan latihan pemulihan perlu dilakukan secara rutin.
4. Penguatan Respons Cepat terhadap Insiden Keamanan: Tim respons insiden yang sudah dibentuk perlu diperkuat untuk memastikan kesiapan merespons setiap insiden keamanan dengan cepat dan efektif. Rapat koordinasi segera setelah menerima laporan insiden harus terus dilakukan dan ditingkatkan untuk mengambil tindakan yang tepat dan cepat.
5. Penegakan Disiplin dan Pengendalian Internal: Tindakan disipliner terhadap kelalaian dan pelanggaran kebijakan keamanan informasi perlu diterapkan. Audit internal secara rutin harus dilakukan untuk mengidentifikasi dan memperbaiki kelemahan dalam sistem keamanan guna mencegah ancaman dari dalam *(insider threat)*.
6. Pengembangan *Business Continuity Plan* (BCP): *Business continuity plan* (BCP) yang solid harus disiapkan untuk memastikan operasional tetap berjalan meski terjadi insiden. Evaluasi dan pembaruan rencana kelangsungan bisnis perlu dilakukan secara berkala untuk menyesuaikan dengan perkembangan teknologi dan ancaman baru.

KESIMPULAN

Berdasarkan hasil analisis Matriks Penilaian Budaya Keamanan Siber dan Matriks Penilaian Budaya Nasional Hofstede, dapat disimpulkan beberapa poin penting sebagai berikut:

Partisipasi karyawan dalam menjaga keamanan informasi masih rendah, menunjukkan perlunya program pelatihan yang lebih intensif dan partisipatif. Dalam konteks budaya nasional dengan jarak kekuasaan tinggi, dukungan dari manajemen puncak sangat penting untuk keberhasilan program ini.

Terjadi kelalaian SDM dalam menonaktifkan fitur keamanan yang menunjukkan kurangnya kepatuhan terhadap standar keamanan. Kebijakan yang ketat dan rinci harus diterapkan, terutama di lingkungan yang memiliki tingkat penghindaran ketidakpastian yang tinggi. Respons cepat yang dilakukan oleh Kepala BSSN menunjukkan pentingnya pengambilan keputusan cepat dan tegas dalam menghadapi insiden keamanan. Budaya maskulin yang menekankan pencapaian hasil dan tindakan tegas sangat mendukung pendekatan ini.

Ketiadaan data cadangan di PDNS 2 menyoroti pentingnya sistem *backup* yang komprehensif. Implementasi *disaster recovery plan* (DRP) yang solid harus menjadi prioritas untuk meningkatkan ketahanan terhadap serangan siber. Investasi dalam audit digital forensik dan latihan simulasi insiden dan pemulihan menunjukkan orientasi jangka panjang yang baik. Organisasi harus terus mengembangkan strategi keamanan yang proaktif dan berkelanjutan untuk menghadapi ancaman di masa depan.

Tindakan tegas terhadap pelanggaran dan kelalaian keamanan informasi menunjukkan budaya pengendalian yang kuat. Audit internal rutin dan penegakan disiplin yang ketat diperlukan untuk menjaga integritas dan keamanan sistem informasi.

DAFTAR PUSTAKA

Ahlan, A.R., Lubis, M. dan Lubis, A.R. (2015) "Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures," in *Procedia Computer Science*. Amsterdam: Elsevier B.V., hal. 361–373. Tersedia pada: https://doi.org/10.1016/j.procs.2015.12.151.

AlHogail, A. (2015) "Design and validation of information security culture framework," *Computers in Human Behavior*, 49, hal. 567–575. Tersedia pada: https://doi.org/10.1016/j.chb.2015.03.054.

Ali, T., Al-Khalidi, M. dan Al-Zaidi, R. (2024) "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," *Journal of Computer Information Systems*, hal. 1–28. Tersedia pada: https://doi.org/10.1080/08874417.2024.2329985.

Alraja, M.N., Butt, U.J. dan Abbod, M. (2023) "Information security policies compliance in a global setting: An employee's perspective," *Computers & Security*, 129, hal. 103208. Tersedia pada: https://doi.org/10.1016/j.cose.2023.103208.

Alvarez-Dionisi, L.E. dan Urrego-Baquero, N. (2019) "Implementing a Cybersecurity Culture," *ISACA JOURNAL*, 2, hal. 1–6. Tersedia pada: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture.

Anggraeni, R. (2024a) *DPR Sesali Bertahun-tahun PDNS 2 Tidak Punya Data Cadangan (Backup)*,

Bisnis Tekno. Diedit oleh Leo Dwi Jatmiko. Tersedia pada: https://teknologi.bisnis.com/read/20240627/101/1777675/dpr-sesali-bertahun-tahun-pdns-2-tidak-punya-data-cadangan-backup (Diakses: 24 Juli 2024).

Anggraeni, R. (2024b) *Server PDNS Down, BSSN Lakukan Audit Digital Forensik*, *Bisnis Tekno*. Tersedia pada: https://teknologi.bisnis.com/read/20240627/101/1777617/server-pdns-down-bssn-lakukan-audit-digital-forensik (Diakses: 24 Juli 2024).

Aranditio, S. (2024) *Terdampak Peretasan PDN, Apa yang Harus Dilakukan Mahasiswa Penerima Beasiswa KIP Kuliah?*, *Kompas.id*. Tersedia pada: https://www.kompas.id/baca/humaniora/2024/07/01/kemendikbudristek-pastikan-data-pokok-pendidikan-aman-dari-peretasan-pdn (Diakses: 24 Juli 2024).

Ashraf, S. (2005) "Organization Need and Everyone's Responsibility Information Security Awareness." SANS Institute, hal. 21. Tersedia pada: https://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113#:~:text=Information Security Awareness is user's,like confidentiality%2C integrity and availability.

Ayanwale, M.A. *et al.* (2023) "A Structural Equation Approach and Modelling of Pre-service Teachers' Perspectives of Cybersecurity Education," *Education and Information Technologies* [Preprint]. Tersedia pada: https://doi.org/10.1007/s10639-023-11973-5.

Bhagat, S. dan Pravin, D.P. (2023) "Cybersecurity Awareness and Adaptive Behavior: Does Prior Exposure Lead to Adaptive Behavior?," in *AMCIS 2023 Proceedings*. Panama City: AIS Electronic Library (AISel), hal. 23.

Bloomberg Technoz (2024) *Kelalaian Tata Kelola Pusat Data (PDN), Minta Maaf Tak Cukup*, *Bloomberg Technoz*. Tersedia pada: https://www.bloombergtechnoz.com/detail-news/42718/kelalaian-tata-kelola-pusat-data-pdn-minta-maaf-tak-cukup (Diakses: 24 Juli 2024).

CNN Indonesia (2024a) *Imbas Peretasan PDNS, Pemerintah Godok Aturan Kewajiban Backup Data*, *CNN Indonesia*. Tersedia pada: https://www.cnnindonesia.com/teknologi/20240710091916-192-1119505/imbas-peretasan-pdns-pemerintah-godok-aturan-kewajiban-backup-data (Diakses: 24 Juli 2024).

CNN Indonesia (2024b) *Insiden Peretasan PDNS 2, Pakar Sorot Kualitas SDM Indonesia*, *CNN Indonesia*. Tersedia pada: https://www.cnnindonesia.com/teknologi/20240626110919-192-1114286/insiden-peretasan-pdns-2-pakar-sorot-kualitas-sdm-indonesia (Diakses: 24 Juli 2024).

CNN Indonesia (2024c) *Update Kasus PDNS 2: Brain Cipher Minta Maaf, Dirjen Aptika Mundur*, *CNN Indonesia*. Tersedia pada: https://www.cnnindonesia.com/teknologi/20240705142613-192-1117995/update-kasus-pdns-2-brain-cipher-minta-maaf-dirjen-aptika-mundur/2 (Diakses: 24 Juli 2024).

D'Arcy, J., Hovav, A. dan Galletta, D. (2009) "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, 20(1), hal. 79–98. Tersedia pada:

https://doi.org/10.1287/isre.1070.0160.

EC-Council (2022) *Ethical Hacking and Countermeasures Academia Series Version 12*. Albuquerque: EC-Council New Mexico.

Fadilah, K. (2024) *Pemerintah Bakal Siapkan 4 Lapis Backup Data Usai PDNS Diretas*, *detik*News. Tersedia pada: https://news.detik.com/berita/d-7417288/pemerintah-bakal-siapkan-4-lapis-backup-data-usai-pdns-diretas (Diakses: 24 Juli 2024).

Hadyan, R. (2024) *Password Disebar Karyawan Picu Serangan Siber ke PDNS 2, Bagaimana Mitigasinya?*, *Investor Trust*. Diedit oleh F.F.S. Putra. Tersedia pada: https://investortrust.id/news/password-disebar-karyawan-picu-serangan-siber-ke-pdns-2-bagaimana-mitigasinya (Diakses: 24 Juli 2024).

Harper, J.W. (2023) "Cybersecurity: A review of human-based behavior and best practices to mitigate risk." MACON: School of Computing Faculty of Middle Georgia State University, hal. 1–9. Tersedia pada: https://comp.mga.edu/static/media/doctoralpapers/2023_Harper_0516152313.pdf.

Hofstede, G., Hofstede, G.J. dan Minkov, M. (2010) *Cultures and Organizations Software of The Mind: Intercultural Cooperation and Its Importance for Survival*. The McGraw-Hill Companies, Inc.

Hofstede, G. dan Minkov, M. (2010) "Long- versus short-term orientation: new perspectives," *Asia Pacific Business Review*, 16(4), hal. 493–504. Tersedia pada: https://doi.org/10.1080/13602381003637609.

Katsantonis, M.N. *et al.* (2023) "Cyber range design framework for cyber security education and training," *International Journal of Information Security*, 22(4), hal. 1005–1027. Tersedia pada: https://doi.org/10.1007/s10207-023-00680-4.

Kure, E. (2024) *Peretasan PDNS 2 Diduga Ulah Oknum Karyawan Lintasarta, Berhenti Kerja Agustus 2021 dan Mulai Bocorkan Data 11 Oktober 2022*, *Berita Satu*. Diedit oleh AD. Tersedia pada: https://www.beritasatu.com/ekonomi/2827333/peretasan-pdns-2-diduga-ulah-oknum-karyawan-lintasarta-berhenti-kerja-agustus-2021-dan-mulai-bocorkan-data-11-oktober-2022 (Diakses: 24 Juli 2024).

Kwon, R. *et al.* (2020) "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," in *2020 Resilience Week (RWS)*. Salt Lake: IEEE, hal. 106–112. Tersedia pada: https://doi.org/10.1109/RWS50334.2020.9241271.

Luthfiani, D. (2024) *Peretas Pusat Data Nasional Minta Tebusan Rp 131 Miliar*, *Tempo*. Diedit oleh R. Paraqbueq. Tersedia pada: https://nasional.tempo.co/read/1883534/peretas-pusat-data-nasional-minta-tebusan-rp-131-miliar (Diakses: 24 Juli 2024).

Merriam, S.B. (2009) *Qualitative Research A Guide to Design and Implementation*. San Francisco: Jossey-Bass. Tersedia pada: https://www.wiley.com/en-us/Qualitative+Research%3A+A+Guide+to+Design+and+Implementation%2C+4th+Edition-p-9781119003618.

Mikuletič, S. *et al.* (2024) "Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees," *Computers*

& Security, 136, hal. 103489. Tersedia pada: https://doi.org/10.1016/j.cose.2023.103489.

Molle, S.S. *et al.* (2024) "Pengaruh Dimensi Budaya Nasional Hofstede terhadap Kinerja Pegawai dalam Pengelolaan Keuangan di Pemerintah Kota Kupang," *Jurnal Ilmiah Universitas Batanghari Jambi*, 24(2), hal. 1683–1691. Tersedia pada: http://ji.unbari.ac.id/index.php/ilmiah/article/view/4963.

Niemimaa, M. (2024) "Incorrect Compliance and Correct Noncompliance with Information Security Policies: A Framework of Rule-Related Information Security Behaviour," *Computers & Security*, hal. 103986. Tersedia pada: https://doi.org/10.1016/j.cose.2024.103986.

Oltsik, J. (2024) *Improving cybersecurity culture: A priority in the year of the CISO*, *CSO*. Tersedia pada: https://www.csoonline.com/article/1298541/improving-cybersecurity-culture-a-priority-in-the-year-of-the-ciso.html#:~:text="The concept of cybersecurity culture,people's behavior with information technologies. (Diakses: 24 Juli 2024).

Pratiwi, M.I. (2017) *IMPLEMENTASI GAYA KEPEMIMPINAN PATERNALISTIK (STUDI KASUS PT JASA RAHARJA PERSERO CABANG JAWA TENGAH)*. Universitas Diponegoro. Tersedia pada: https://repofeb.undip.ac.id/9649/.

Puspitasari, D. (2024) *Tata Kelola PDN Kacau, Harus Sanksi Tak Cuma Minta Maaf*, *KABARBURSA.COM*. Tersedia pada: https://www.kabarbursa.com/berita-pilihan/63443/tata-kelola-pdn-kacau-harus-sanksi-tak-cuma-minta-maaf (Diakses: 24 Juli 2024).

Rahmawati, D. (2024) *BSSN Jelaskan Upaya Pulihkan Layanan Imigrasi Usai PDNS Kena Ransomware*, *detikNews*. Tersedia pada: https://news.detik.com/berita/d-7412027/bssn-jelaskan-upaya-pulihkan-layanan-imigrasi-usai-pdns-kena-ransomware (Diakses: 24 Juli 2024).

Rochman, F. (2024) *Dirjen Aptika mundur setelah insiden serangan siber terhadap PDNS 2*, *Antara Kuala Lumpur*. Diedit oleh V.P. Setyorini. Antara. Tersedia pada: https://kl.antaranews.com/berita/26115/dirjen-aptika-mundur-setelah-insiden-serangan-siber-terhadap-pdns-2 (Diakses: 24 Juli 2024).

Saeed, S. (2023) "Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia," *Sustainability*, 15(12), hal. 9426. Tersedia pada: https://doi.org/10.3390/su15129426.

Safitri, E. (2024) *Jokowi Perintahkan BPKP Audit Pusat Data Nasional Buntut Peretasan*, *detikNews*. Tersedia pada: https://news.detik.com/berita/d-7414588/jokowi-perintahkan-bpkp-audit-pusat-data-nasional-buntut-peretasan (Diakses: 24 Juli 2024).

Sari, D.R. dan Dirgahayu, T. (2017) "Adopsi Theory of Planned Behavior Untuk Pengembangan Model Pengaruh Budaya Terhadap Penggunaan E-Commerce," *Jurnal Buana Informatika*, 8(2), hal. 67–76. Tersedia pada: https://ojs.uajy.ac.id/index.php/jbi/article/view/1078.

Tenzin, S., McGill, T. dan Dixon, M. (2024) "An Investigation of the Factors That Influence Information Security Culture in Government Organizations in Bhutan," *Journal of*

Global Information Technology Management, 27(1), hal. 37–62. Tersedia pada: https://doi.org/10.1080/1097198X.2023.2297634.

Tsoeu, M.A. dan da Veiga, A. (2022) "A Cyber4Dev Security Culture Model," in T. Guarda, F. Portela, dan M.F. Augusto (ed.) *Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2022. Communications in Computer and Information Science*. Cham: Springer Nature Switzerland, hal. 339–351. Tersedia pada: https://link.springer.com/chapter/10.1007/978-3-031-20316-9_26.

Wakang, A.A. (2024) *Beranda Nasional PDNS Diretas, PPI Dunia Sarankan Buat Simulasi Rutin Kesiapan Hadapi Serangan Siber*, *Tempo*. Diedit oleh I. Hamdi. Tersedia pada: https://nasional.tempo.co/read/1886811/pdns-diretas-ppi-dunia-sarankan-buat-simulasi-rutin-kesiapan-hadapi-serangan-siber.

Wardani, D.K. dan Nurainun'nisa, N. (2024) "Analisis Perilaku Kecurangan Akademik Pada Mahasiswa Akuntansi Menggunakan Konsep Budaya Hofstede," *Relasi: Jurnal Ekonomi*, 20(1), hal. 44–58. Tersedia pada: http://jurnal.itsm.ac.id/index.php/relasi/article/view/698.