CONFLUENCE
Journal of Business, Economics & Governance

E ISSN 3124-792X

Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

PENGARUH KEPEMIMPINAN OTORITER DAN TEKANAN KERJA TERHADAP TINDAKAN *CYBERCRIME* YANG DILAKUKAN KARYAWAN DI LINGKUNGAN ORGANISASI

[1]Indah Sari Liza Lubis, [2] Donny Setha
[1,2] Fakultas Bisnis dan Humaniora, Universitas Tjut Nyak Dhien
Email Author: indah99_psycho@yahoo.com

Abstract
This study aims to analyze the influence of authoritarian leadership and work pressure on cybercrime committed by employees in an organizational environment. Cybercrime is a form of deviant behavior that utilizes information technology and computer systems that can cause harm to the organization. Organizational and psychological factors of employees are suspected to be the causes of this behavior, including authoritarian leadership and work pressure. This study uses a quantitative approach with an explanatory research method. The population in this study are employees of the organization that is the object of research. Data collection techniques were carried out through the distribution of questionnaires. Data analysis used validity tests, reliability tests, classical assumption tests, multiple linear regression analysis, t-tests, F-tests, and coefficients of determination with the help of the SPSS program. The results of the study indicate that authoritarian leadership has no significant effect on cybercrime. Work pressure has a positive and significant effect on cybercrime. Simultaneously, authoritarian leadership and work pressure have a significant effect on cybercrime. The Adjusted R Square value of 0.624 indicates that 62.4% of the variation in cybercrime can be explained by authoritarian leadership and work pressure, while the remaining 37.6% is explained by other factors outside the study.
Keywords: *Authoritarian Leadership, Cybercrime, Employees, Organization, Work Pressure*

Abstrak
Penelitian ini bertujuan untuk menganalisis pengaruh kepemimpinan otoriter dan tekanan kerja terhadap tindakan *cybercrime* yang dilakukan karyawan di lingkungan organisasi. *Cybercrime* merupakan salah satu bentuk perilaku menyimpang yang memanfaatkan teknologi informasi dan sistem komputer yang dapat menimbulkan kerugian bagi organisasi. Faktor organisasi dan faktor psikologis karyawan diduga menjadi penyebab munculnya perilaku tersebut, di antaranya kepemimpinan otoriter dan tekanan kerja. Penelitian ini menggunakan pendekatan kuantitatif dengan metode penelitian eksplanatori. Populasi dalam penelitian ini adalah karyawan organisasi yang menjadi objek penelitian. Teknik pengumpulan data dilakukan melalui penyebaran kuesioner. Analisis data menggunakan uji validitas, uji reliabilitas, uji asumsi klasik, analisis regresi linier berganda, uji t, uji F, dan koefisien determinasi dengan bantuan program SPSS. Hasil penelitian menunjukkan bahwa kepemimpinan otoriter tidak berpengaruh signifikan terhadap tindakan *cybercrime*. Tekanan kerja berpengaruh positif dan signifikan terhadap tindakan *cybercrime*. Secara simultan, kepemimpinan otoriter dan tekanan kerja berpengaruh signifikan terhadap tindakan *cybercrime*. Nilai Adjusted R Square sebesar 0,624 menunjukkan bahwa 62,4% variasi tindakan *cybercrime* dapat dijelaskan oleh kepemimpinan otoriter dan tekanan kerja, sedangkan sisanya sebesar 37,6% dijelaskan oleh faktor lain di luar penelitian.
Kata Kunci: Kepemimpinan Otoriter, Karyawan, Organisasi, Tekanan Kerja, Tindakan *Cybercrime*

PENDAHULUAN

Transformasi digital telah meningkatkan efektivitas operasional organisasi, namun pada saat yang sama memunculkan berbagai risiko keamanan informasi yang berasal dari perilaku karyawan. Salah satu ancaman yang semakin mendapatkan perhatian adalah tindakan *cybercrime* yang dilakukan oleh karyawan atau *insider threat*. Tindakan *cybercrime* dalam organisasi mencakup penyalahgunaan akses sistem, pencurian data, penyebaran *malware*,

kebocoran informasi perusahaan, hingga penggunaan internet untuk aktivitas yang merugikan organisasi (Zhang et al., 2022).

Berbagai penelitian menunjukkan bahwa faktor manusia menjadi salah satu penyebab utama insiden keamanan siber dalam organisasi. Ancaman dari orang dalam bahkan dinilai lebih sulit dideteksi dibandingkan serangan dari pihak eksternal karena pelaku memiliki akses yang sah terhadap sistem organisasi (Jones, 2024).

Secara makro, perkembangan teknologi digital telah menyebabkan peningkatan kasus kejahatan siber di berbagai sektor industri. Laporan keamanan siber menunjukkan bahwa ancaman *insider threat* terus meningkat dan menjadi salah satu penyebab utama kebocoran data organisasi. Pada tahun 2025, sekitar 32% insiden kehilangan data organisasi di dunia melibatkan pelaku dari dalam organisasi atau karyawan yang memiliki akses terhadap sistem perusahaan. Kondisi ini menunjukkan bahwa perilaku karyawan merupakan faktor penting dalam upaya menjaga keamanan informasi organisasi (Loten, 2026).

Fenomena *cybercrime* karyawan tidak hanya berkaitan dengan kemampuan teknis, tetapi juga dipengaruhi oleh faktor psikologis dan lingkungan kerja. Salah satu faktor yang diduga berpengaruh adalah kepemimpinan otoriter. Kepemimpinan otoriter ditandai dengan pengambilan keputusan yang terpusat, kontrol yang ketat, tuntutan kepatuhan tinggi, serta minimnya partisipasi bawahan dalam proses organisasi.

Penelitian menunjukkan bahwa kepemimpinan otoriter dapat meningkatkan kelelahan emosional karyawan yang kemudian mendorong munculnya perilaku menyimpang berbasis teknologi seperti *cyberloafing* dan penyalahgunaan internet di tempat kerja (Zhang, Yajun, 2022).

Selain kepemimpinan otoriter, tekanan kerja juga menjadi faktor yang berpotensi memicu tindakan *cybercrime*. Tingginya beban kerja, tuntutan target, tekanan waktu, dan konflik pekerjaan dapat menyebabkan stres kerja yang berdampak pada penurunan kontrol diri karyawan. Dalam kondisi tersebut, sebagian karyawan berpotensi melakukan tindakan menyimpang sebagai bentuk pelampiasan atau mekanisme *coping* terhadap tekanan yang dialami. Penelitian terdahulu menunjukkan bahwa tekanan kerja dan kelelahan emosional berhubungan dengan meningkatnya perilaku *cyberloafing*, penyalahgunaan teknologi, dan perilaku kontraproduktif lainnya di lingkungan kerja (Song, 2023a).

Di Indonesia, masih ditemukan berbagai kasus tindakan *cybercrime*, seperti penyalahgunaan akses sistem oleh karyawan, kebocoran data pelanggan, penggunaan perangkat organisasi untuk aktivitas pribadi, serta tindakan pelanggaran keamanan informasi

yang dilakukan oleh pegawai internal. penelitan ini penting karena . Pada tahun 2024, Polda Metro Jaya mengungkap kasus mantan karyawan bank digital yang menyalahgunakan kewenangannya sebagai *contact center specialist* untuk membuka blokir rekening nasabah secara ilegal. Pelaku melakukan persetujuan pembukaan blokir terhadap 112 rekening dan memindahkan dana sekitar Rp1,39 miliar ke rekening yang telah disiapkan sebelumnya. Kasus ini menunjukkan bahwa akses yang dimiliki karyawan dapat disalahgunakan untuk melakukan tindakan *cybercrime* dari dalam organisasi (Djailani, 2024).

Dari hasil observasi awal 30 karyawan bank pemerintah di kota Medan sebesar 21 karyawan melakukan tindakan *cybercrime* karena kepemimpinan otoriter yang selalu membuat karyawan tertekan, sehingga tidak mampu mengontrol diri dan dapat menyalahgunakan akses sistem perbankan, pencurian atau pengalihan dana nasabah, manipulasi data transaksi elektronik, penyalahgunaan jaringan internet perusahaan untuk aktivitas ilegal dan *Cyberloafing* yang berkembang menjadi pelanggaran keamanan informasi. Selain itu, 22 karyawan melakukan tindakan *cybercrime* karena lingkungan kerja tekanan kerja dan tuntutan kerja yang tinggi, sehingga mengalami stress kerja

Penelitian ini menjadi penting karena kepemimpinan otoriter dan tekanan kerja merupakan dua faktor yang sering dijumpai dalam lingkungan organisasi, namun pengaruh keduanya terhadap tindakan *cybercrime* karyawan masih relatif jarang diteliti. Padahal, perilaku cybercrime dapat menimbulkan kerugian finansial, kebocoran data, gangguan operasional, serta menurunkan reputasi organisasi. Sebagian besar studi terdahulu, seperti penelitian (Peng, Jian, 2023) lebih banyak membahas *cyberloafing*, keamanan informasi, dan insider threat secara terpisah. Masih terbatas penelitian yang secara simultan menguji pengaruh kepemimpinan otoriter dan tekanan kerja terhadap tindakan *cybercrime* yang dilakukan karyawan dalam konteks organisasi. Kebaruan penelitian ini terletak pada penggunaan variabel tindakan cybercrime karyawan sebagai variabel dependen yang masih jarang diteliti dalam kajian manajemen sumber daya manusia, pengintegrasian dua variabel perilaku organisasi, yaitu kepemimpinan otoriter dan tekanan kerja, dalam menjelaskan tindakan *cybercrime* internal, sedangkan penelitian (Zhang, Yajun, 2022) masih didominasi pembahasan *cyberloafing* dibandingkan tindakan *cybercrime* karyawan secara langsung studi mengenai kepemimpinan otoriter lebih banyak dikaitkan dengan kelelahan emosional dan *cyberloafing*, belum banyak yang menghubungkannya dengan *cybercrime* internal, serta Penelitian tekanan kerja umumnya menempatkan *cyberloafing* sebagai variabel dependen, bukan tindakan *cybercrime*.

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

TINJAUAN PUSTAKA

Kepemimpinan Otoriter

Kepemimpinan otoriter (*authoritarian leadership*) adalah gaya kepemimpinan yang menempatkan seluruh kewenangan dan pengambilan keputusan pada pemimpin, sementara bawahan dituntut untuk mematuhi instruksi tanpa banyak dilibatkan dalam proses pengambilan keputusan. Pemimpin mengendalikan aktivitas kerja secara ketat, menetapkan aturan yang harus dipatuhi, serta memberikan sedikit kesempatan kepada karyawan untuk menyampaikan pendapat atau berpartisipasi dalam penentuan kebijakan organisasi (Zhang, Yajun, 2022). Kepemimpinan otoriter merupakan perilaku pemimpin yang menegaskan otoritas absolut, mengontrol bawahan secara ketat, serta menuntut kepatuhan tanpa syarat dari para pengikutnya (Song, 2023a). Kepemimpinan otoriter adalah gaya kepemimpinan yang menekankan kontrol penuh pemimpin terhadap pekerjaan dan perilaku bawahan, dengan komunikasi yang cenderung satu arah dari atasan kepada bawahan (Blau and Stephens, 2025). Indikator kepemimpinan otoriter menurut (Robbins & Judge, 2022), yaitu sentralisasi pengambilan keputusan, kekuasaan terpusat pada pemimpin, partisipasi bawahan yang rendah, pengawasan kerja yang ketat, komunikasi satu arah, penekanan pada kepatuhan, pengendalian perilaku bawahan, pemberian instruksi yang dominan, penegakan disiplin yang tinggi dan pemberian sanksi terhadap pelanggaran.

Tekanan Kerja

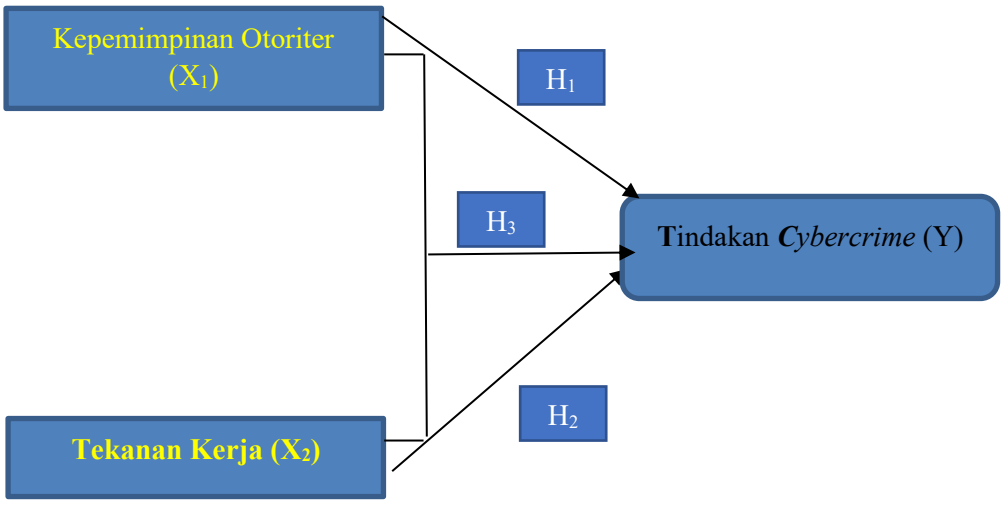
Tekanan kerja (*job stress* atau *work pressure*) adalah kondisi ketika karyawan menghadapi tuntutan pekerjaan yang melebihi kemampuan, sumber daya, atau kapasitas yang dimiliki sehingga menimbulkan ketegangan fisik, psikologis, dan emosional (Rizqi and Swasti, 2025). Tekanan kerja merupakan kondisi yang timbul akibat interaksi antara karakteristik pekerjaan dengan karakteristik individu yang menyebabkan perubahan pada kondisi psikologis maupun fisiologis pekerja (Kwala and Agoyi, 2025). Indikator tekanan kerja menurut (Jones, 2024) adalah beban kerja berlebihan, tekanan waktu, tuntutan kinerja yang tinggi, konflik peran, ketidakjelasan peran, kurangnya dukungan atasan, hubungan kerja yang Kurang harmonis, kurangnya kontrol terhadap pekerjaan, ketidakamanan pekerjaan dan perubahan organisasi yang cepat.

Tindakan *Cybercrime*

Tindakan *cybercrime* adalah segala bentuk perilaku ilegal atau penyalahgunaan teknologi informasi dan sistem komputer yang dilakukan untuk memperoleh keuntungan pribadi, merugikan pihak lain, mencuri informasi, mengganggu sistem, atau melanggar

kebijakan keamanan organisasi (Gelman, Haywood, 2023). Dalam konteks organisasi, tindakan *cybercrime* tidak hanya dilakukan oleh pihak eksternal (hacker), tetapi juga oleh karyawan internal (*insider threat*) yang memiliki akses sah terhadap sistem informasi perusahaan (Shikonde and Nkongolo, 2025). Indikator tindakan *cybercrime* karyawan menurut (Peng, Jian, 2023) adalah mengakses data atau informasi organisasi tanpa kewenangan yang jelas, menggunakan akun atau hak akses milik orang lain tanpa izin, menyalin atau menyimpan data organisasi untuk kepentingan pribadi, membagikan informasi rahasia organisasi kepada pihak yang tidak berwenang, mengubah atau memanipulasi data dalam sistem tanpa persetujuan, menghapus data atau dokumen digital tanpa prosedur yang berlaku, menggunakan perangkat atau jaringan organisasi untuk aktivitas ilegal, mengunduh perangkat lunak atau file yang berpotensi mengancam keamanan sistem organisasi, mengabaikan prosedur keamanan informasi yang telah ditetapkan organisasi dan memanfaatkan kelemahan sistem organisasi untuk memperoleh keuntungan pribadi.

Sesuai permasalahan dan tinjauan pustaka, maka kerangka konseptual penelitian adalah sebagai berikut:



Gambar 1 Kerangka Konseptual

Adapun penjabaran kerangka konseptual melalui hipotesis penelitian adalah sebagai berikut:

Hubungan Kepemimpinan Otoriter terhadap Tindakan *Cybercrime* Karyawan Bank Pemerintah

Menurut teori kepemimpinan, gaya kepemimpinan otoriter menekankan sentralisasi wewenang pada pemimpin, di mana seluruh keputusan strategis maupun operasional ditentukan oleh atasan. Karyawan diharapkan melaksanakan instruksi sesuai arahan tanpa

banyak diskusi atau negosiasi. Pola kepemimpinan ini umumnya disertai dengan pengawasan yang intensif, standar kerja yang ketat, serta pemberian sanksi apabila terjadi penyimpangan dari aturan yang telah ditetapkan (Robbins & Judge, 2022). Gaya kepemimpinan otoriter berpengaruh terhadap tindakan *cybercrime* karyawan, dimana menurut temuan penelitian (Zhang, 2022) menunjukkan bahwa kepemimpinan otoriter berpengaruh positif terhadap berbagai perilaku kerja yang menyimpang, termasuk *cyberloafing* melalui kelelahan emosional sebagai variabel mediasi. Meskipun *cyberloafing* berbeda dengan *cybercrime*, keduanya merupakan bentuk penyalahgunaan teknologi di lingkungan kerja sehingga memberikan dasar empiris bahwa kepemimpinan otoriter dapat meningkatkan risiko perilaku digital yang menyimpang.

H_1: Kepemimpinan otoriter berpengaruh terhadap tindakan *cybercrime* karyawan bank pemerintah.

Hubungan Tekanan Kerja terhadap Tindakan *Cybercrime* Karyawan Bank Pemerintah

Menurut teori stres kerja dari Richard Lazarus dan Susan Folkman, tekanan kerja muncul ketika tuntutan pekerjaan melebihi kemampuan individu untuk mengatasinya. Tekanan tersebut dapat berasal dari beban kerja yang tinggi, target yang sulit dicapai, keterbatasan waktu, konflik peran, maupun tanggung jawab pekerjaan yang besar. Tekanan kerja berpengaruh terhadap tindakan *cybercrime* karyawan, dimana menurut temuan penelitian (Gelman, Haywood, 2023) menyatakan semakin tinggi tekanan kerja yang dialami karyawan, semakin besar kemungkinan munculnya tindakan *cybercrime* sebagai bentuk perilaku kontraproduktif di lingkungan organisasi.

H_2: Tekanan kerja berpengaruh terhadap tindakan *cybercrime* karyawan bank pemerintah

Hubungan Kepemimpinan Otoriter dan Tekanan Kerja terhadap Tindakan *Cybercrime* Karyawan Bank Pemerintah

Secara konseptual, kepemimpinan otoriter merupakan salah satu faktor organisasi yang dapat meningkatkan tekanan kerja. Pemimpin yang menerapkan kontrol secara berlebihan, memberikan target tanpa melibatkan bawahan dalam pengambilan keputusan, serta menerapkan komunikasi yang kaku dapat menyebabkan karyawan merasa tertekan secara psikologis. Gaya kepemimpinan otoriter dan tekanan kerja berpengaruh terhadap tindakan *cybercrime* karyawan. Hal ini sesuai temuan penelitian (Kwala and Agoyi, 2025) menemukan adanya hubungan positif yang signifikan antara persepsi terhadap gaya kepemimpinan otoriter

dan tekanan kerja. Artinya, semakin tinggi persepsi karyawan terhadap kepemimpinan otoriter, semakin tinggi pula tekanan kerja yang mereka rasakan.

H_3: Kepemimpinan otoriter dan tekanan kerja berpengaruh terhadap tindakan *cybercrime* karyawan bank pemerintah.

METODE PENELITIAN

Metode penelitian ini akan menggunakan metode deskriptif kuantitatif, dimana menurut (Ghozali, 2021) metode deskriptif kuantitatif merupakan pendekatan penelitian yang bertujuan untuk menggambarkan, menjelaskan, dan menganalisis fenomena yang terjadi berdasarkan data numerik yang diperoleh dari responden melalui instrumen penelitian yang terstruktur.

Populasi dalam penelitian ini adalah 38.874 karyawan Bank Mandiri di Indonesia Tahun 2025, dimana metode pengambilan sampelnya dilakukan dengan menggunakan metode *accidental sampling*, dimana menurut (Katto dan Pratama, 2023) metode pengambilan sampel menggunakan *accidental sampling* adalah merupakan metode pengambilan sampel yang sampelnya ada di tempat atau objek penelitian (Katto dan Pratama, 2023). Pengambilan sampel dilakukan menggunakan rumus slovin yang perhitungannya adalah:

$n = N / (1 + Ne^2) = 38.874 / (1 + 38.874 \times 0.1^2) = 99{,}74 = 99$ karyawan Bank Mandiri di Indonesia Tahun 2025, dengan *margin of error* 10%, dimana *margin of error* 10% digunakan karena menunjukkan tingkat kesalahan yang masih dapat diterima antara hasil sampel dengan kondisi populasi yang sebenarnya.

Adapun pengambilan data dilakukan dengan kuesioner melalui penyebaran pertanyaan melalui *g-form* yang disebarkan melalui instagram dan studi dokumentasi melalui pengambilan sumber penelitian dari website. teknik analisis data yang digunakan melalui uji regresi linier berganda, seperti uji normalitas, uji multikolinearitas, uji heteroskedastisitas, persamaan regresi linier berganda, uji t (parsial), uji F (simultan) dan uji koefisien determinasi.

Dalam penelitian kuantitatif, keabsahan data dilakukan melalui uji validitas dan uji reliabilitas instrumen penelitian. Instrumen penelitian yang digunakan dalam penelitian ini adalah kuesioner (angket) yang disusun berdasarkan indikator dari masing-masing variabel penelitian. Adapun definisi operasional variabel dan indikator dari masing-masing variabel dapat dilihat pada tabel berikut:

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

Tabel 1 Definisi Operasional Variabel dan Indikatornya

No	Variabel	Definisi Operasional	Indikator
1	Kepemimpinan Otoriter (X_1)	Gaya kepemimpinan yang menekankan kontrol penuh pemimpin terhadap pekerjaan dan perilaku bawahan, dengan komunikasi yang cenderung satu arah dari atasan kepada bawahan	Sentralisasi pengambilan keputusan, kekuasaan terpusat pada pemimpin, partisipasi bawahan yang rendah, pengawasan kerja yang ketat, komunikasi satu arah, penekanan pada kepatuhan, pengendalian perilaku bawahan, pemberian instruksi yang dominan, penegakan disiplin yang tinggi dan pemberian sanksi terhadap pelanggaran
2	Tekanan Kerja (X_2)	Kondisi yang timbul akibat interaksi antara karakteristik pekerjaan dengan karakteristik individu yang menyebabkan perubahan pada kondisi psikologis maupun fisiologis pekerja	Beban kerja berlebihan, tekanan waktu, tuntutan kinerja yang tinggi, konflik peran, ketidakjelasan peran, kurangnya dukungan atasan, hubungan kerja yang Kurang harmonis, kurangnya kontrol terhadap pekerjaan, ketidakamanan pekerjaan dan perubahan organisasi yang cepat
3	Tekanan Kerja (Y)	Segala bentuk perilaku ilegal atau penyalahgunaan teknologi informasi dan sistem komputer yang dilakukan untuk memperoleh keuntungan pribadi, merugikan pihak lain, mencuri informasi, mengganggu sistem, atau melanggar kebijakan keamanan organisasi	Mengakses data atau informasi organisasi tanpa kewenangan yang jelas, menggunakan akun atau hak akses milik orang lain tanpa izin, menyalin atau menyimpan data organisasi untuk kepentingan pribadi, membagikan informasi rahasia organisasi kepada pihak yang tidak berwenang, mengubah atau memanipulasi data dalam sistem tanpa persetujuan, menghapus data atau dokumen digital tanpa prosedur yang berlaku, menggunakan perangkat atau jaringan organisasi untuk aktivitas ilegal, mengunduh perangkat lunak atau file yang berpotensi mengancam keamanan sistem organisasi, mengabaikan prosedur keamanan informasi yang telah ditetapkan organisasi dan memanfaatkan kelemahan sistem organisasi untuk memperoleh keuntungan pribadi

Sumber: Peneliti (2026)

Penelitian ini dilaksanakan di bank pemerintah di Indonesia yang dilaksanakan bulan Maret sampai Mei 2026. Pemilihan lokasi penelitian didasarkan pada pertimbangan bahwa organisasi tersebut telah menerapkan sistem teknologi informasi dalam pelaksanaan aktivitas

operasionalnya, sehingga memungkinkan terjadinya interaksi karyawan dengan berbagai perangkat dan sistem digital yang relevan dengan variabel tindakan *cybercrime*. Selain itu, organisasi tersebut memiliki karakteristik lingkungan kerja yang memungkinkan munculnya fenomena kepemimpinan otoriter dan tekanan kerja, sehingga sesuai dengan tujuan penelitian untuk menganalisis pengaruh kedua variabel tersebut terhadap tindakan *cybercrime* yang dilakukan karyawan.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Karakteristik Responden

Tabel 2 Karakteristik Responden Sesuai Jenis Kelamin

Jenis Kelamin	Frekuensi	Persentase (%)
Laki-laki	45	45,5
Perempuan	54	54,5
Total	99	100,00

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Mayoritas responden yang menjawab pertanyaan adalah karyawan Bank Mandiri di Indonesia berjenis kelamin perempuan sebanyak 54 orang (54,5%), sedangkan karyawan laki-laki berjumlah 45 orang (45,5%). Hal ini menunjukkan bahwa komposisi responden didominasi oleh karyawan perempuan.

Tabel 3 Karakteristik Responden Berdasarkan Usia

Usia	Frekuensi	Persentase (%)
21–30 tahun	29	29,3
31–40 tahun	41	41,4
41–50 tahun	20	20,2
>50 tahun	9	9,1
Total	99	100,00

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Sebagian besar responden berusia 31–40 tahun sebanyak 41 orang (41,4%), menunjukkan bahwa mayoritas karyawan Bank Mandiri di Indonesia yang menjawab pertanyaan berada pada usia produktif dan telah memiliki pengalaman kerja yang memadai.

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

Tabel 4 Karakteristik Responden Berdasarkan Pendidikan Terakhir

Pendidikan	Frekuensi	Persentase (%)
Diploma (D3)	16	16,2
Sarjana (S1)	67	67,7
Magister (S2)	16	16,2
Total	99	100,00

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Mayoritas responden karyawan Bank Mandiri di Indonesia yang menjawab pertanyaan memiliki pendidikan terakhir Sarjana (S1), yaitu 67 orang (67,7%), yang menunjukkan bahwa sebagian besar karyawan bank memiliki latar belakang pendidikan tinggi sesuai dengan tuntutan kompetensi di sektor perbankan.

Tabel 5 Karakteristik Responden Berdasarkan Masa Kerja

Masa Kerja	Frekuensi	Persentase (%)
< 5 tahun	23	23,2
5–10 tahun	34	34,3
11–15 tahun	24	24,2
>15 tahun	18	18,2
Total	99	100,00

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Sebagian besar responden karyawan Bank Mandiri di Indonesia yang menjawab pertanyaan memiliki masa kerja 5–10 tahun sebanyak 34 orang (34,4%), yang menunjukkan bahwa responden telah cukup lama bekerja sehingga memahami budaya organisasi dan penggunaan sistem kerja di bank.

Tabel 6 Karakteristik Responden Berdasarkan Lama Menggunakan Sistem Digital Bank

Masa Kerja	Frekuensi	Persentase (%)
< 3 tahun	18	18,2
3–5 tahun	29	29,3
6–10 tahun	34	34,3
>10 tahun	18	18,2
Total	99	100,00

Sumber: Data Diolah Dari Hasil Penelitian, 2026

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

Mayoritas responden karyawan Bank Mandiri di Indonesia yang menjawab pertanyaan telah menggunakan sistem digital bank selama 6–10 tahun sebanyak 34 orang (34,3%). Hal ini menunjukkan bahwa sebagian besar responden telah memiliki pengalaman yang cukup dalam mengoperasikan sistem informasi perbankan, sehingga dapat memberikan penilaian yang baik terhadap variabel kepemimpinan, tekanan kerja, dan perilaku terkait penggunaan sistem digital.

Uji Validitas Variabel Kepemimpinan Otoriter

Tabel 7 Uji Validitas Variabel Kepemimpinan Otoriter

Item Pertanyaan	Nilai r Hitung (*Corrected Total Item Correlations*)	Nilai r Tabel	Keterangan
Q1	.600	0,199	Valid
Q2	.509	0,199	Valid
Q3	.417	0,199	Valid
Q4	.665	0,199	Valid
Q5	.640	0,199	Valid
Q6	.412	0,199	Valid
Q7	.575	0,199	Valid
Q8	.520	0,199	Valid
Q9	.656	0,199	Valid
Q10	.475	0,199	Valid

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Menurut Tabel di atas dapat disimpulkan bahwa item pertanyaan untuk variabel kepemimpinan otoriter dinyatakan valid, karena nilai *Corrected Item-Total Correlation* > Nilai r Tabel 0,199.

Uji Validitas Variabel Tekanan Kerja

Tabel 8 Uji Validitas Variabel Tekanan Kerja

Item Pertanyaan	Nilai r Hitung (*Corrected Total Item Correlations*)	Nilai r Tabel	Keterangan
Q1	.391	0,199	Valid
Q2	.353	0,199	Valid

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

Q3	.643	0,199	Valid
Q4	.557	0,199	Valid
Q5	.722	0,199	Valid
Q6	.544	0,199	Valid
Q7	.610	0,199	Valid
Q8	.654	0,199	Valid
Q9	.681	0,199	Valid
Q10	.590	0,199	Valid

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Seluruh item pernyataan variabel tekanan kerja memiliki nilai *Corrected Item-Total Correlation* > Nilai r Tabel 0,199, sehingga seluruh item dinyatakan valid.

Uji Validitas Variabel Tindakan *Cybercrime*

Tabel 9 Uji Validitas Variabel Tindakan *Cybercrime*

Item Pertanyaan	Nilai r Hitung (*Corrected Total Item Correlations*)	Nilai r Tabel	Keterangan
Q1	.481	0,199	Valid
Q2	.629	0,199	Valid
Q3	.670	0,199	Valid
Q4	.544	0,199	Valid
Q5	.715	0,199	Valid
Q6	.626	0,199	Valid
Q7	.713	0,199	Valid
Q8	.392	0,199	Valid
Q9	.621	0,199	Valid
Q10	.608	0,199	Valid

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Seluruh item pernyataan variabel tindakan *cybercrime* memiliki nilai *Corrected Item-Total Correlation* > Nilai r Tabel 0,199, sehingga seluruh item dinyatakan valid.

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

Uji Reliabilitas

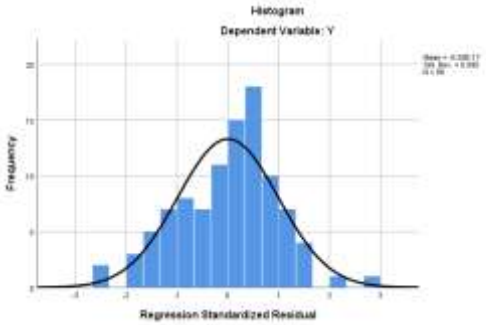
Tabel 10 Uji Reliabilitas Data

Variabel	*Cronbach Alpha*	N of Items	Keterangan
Kepemimpinan Otoriter (X_1)	.809	10	Reliabel
Tekanan Kerja (X_2)	.798	10	Reliabel
Tindakan *Cybercrime* (Y)	.754	10	Reliabel

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Nilai Cronbach's Alpha seluruh variabel lebih besar dari 0,70 sehingga instrumen penelitian dinyatakan reliabel dan dapat digunakan dalam penelitian.

Uji Normalitas



Gambar 2 Diagram Histogram

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Berdasarkan hasil uji normalitas menggunakan grafik Histogram, terlihat bahwa pola distribusi data membentuk kurva menyerupai lonceng (*bell shaped curve*) dan penyebaran frekuensi residual mengikuti pola distribusi normal. Hal ini menunjukkan bahwa residual penelitian terdistribusi secara normal. Dengan demikian, model regresi memenuhi asumsi normalitas sehingga layak digunakan untuk analisis regresi linier berganda.

Uji Multikolinearitas

Tabel 11 Uji Multikolinearitas

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	27.518	4.337		6.345	.000		
X1	-.051	.084	-.060	-.600	.550	.995	1.005
X2	.180	.092	.195	5.953	.004	.995	1.005

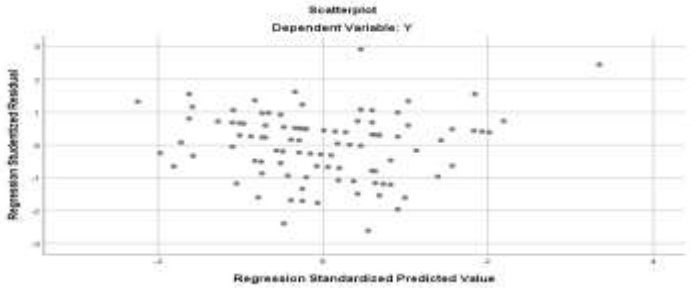
a. Dependent Variable: Y

Sumber: Data Diolah Dari Hasil Penelitian, 2026

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

Nilai Tolerance seluruh variabel > 0,10 dan nilai VIF < 10. Dengan demikian tidak terjadi multikolinearitas dalam model regresi.

Uji Heteroskedastisitas



Gambar 3 Uji Heteroskedastisitas

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Berdasarkan hasil pengolahan data menggunakan diagram Scatterplot, terlihat bahwa titik-titik residual menyebar secara acak di atas dan di bawah angka 0 pada sumbu Y serta tidak membentuk pola tertentu seperti pola bergelombang, menyempit, atau melebar. Penyebaran titik yang acak tersebut menunjukkan bahwa varians residual bersifat konstan. Dengan demikian dapat disimpulkan bahwa model regresi tidak mengalami masalah heteroskedastisitas, sehingga salah satu asumsi klasik dalam analisis regresi linier berganda telah terpenuhi dan model regresi layak digunakan untuk pengujian hipotesis.

Analisis Regresi Linier Berganda

Tabel 12 Analisis Regresi Linier Berganda

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
	B	Std. Error	Beta	t	Sig.	Tolerance	VIF
(Constant)	27.518	4.337		6.345	.000		
X1	-.051	.084	-.060	-.600	.550	.995	1.005
X2	.180	.092	.195	5.953	.004	.995	1.005

a. Dependent Variable: Y

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Berdasarkan hasil pengolahan data diperoleh persamaan regresi:

$$Y = 27.518 - 0{,}051\ X_1 + 0{,}180\ X_2$$

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

1. Konstanta sebesar 27,518 menunjukkan bahwa apabila Kepemimpinan Otoriter dan Tekanan Kerja dianggap konstan, maka nilai Tindakan *Cybercrime* sebesar 27,518.
2. Koefisien Kepemimpinan Otoriter sebesar -0,051 menunjukkan bahwa setiap peningkatan 1 satuan Kepemimpinan Otoriter akan menurunkan Tindakan Cybercrime sebesar 0,051 satuan.
3. Koefisien Tekanan Kerja sebesar 0,180 menunjukkan bahwa setiap peningkatan 1 satuan Tekanan Kerja akan meningkatkan Tindakan *Cybercrime* sebesar 0,180 satuan.

Uji t (Parsial)

Tabel 13 Uji t (Parsial)

Coefficients[a]

	Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
	B	Std. Error	Beta	T	Sig.	Tolerance	VIF
(Constant)	27.518	4.337		6.345	.000		
X1	-.051	.084	-.060	-.600	.550	.995	1.005
X2	.180	.092	.195	5.953	.004	.995	1.005

a. Dependent Variable: Y

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Nilai signifikansi sebesar 0,550 > 1,661 (t-tabel) sehingga Kepemimpinan Otoriter tidak berpengaruh signifikan terhadap Tindakan *Cybercrime*. Dengan demikian hipotesis pertama ditolak. Nilai signifikansi sebesar 0,004 < 0,05 (t-tabel) sehingga Tekanan Kerja berpengaruh positif dan signifikan terhadap Tindakan *Cybercrime*. Dengan demikian hipotesis kedua diterima.

Uji F (Simultan)

Tabel 14 Uji F (Simultan)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	32.840	2	16.420	7.180	.009[b]
	Residual	723.119	96	7.532		
	Total	755.960	98			

a. Dependent Variable: Y

b. Predictors: (Constant), X2, X1

Sumber: Data Diolah Dari Hasil Penelitian, 2026

CONFLUENCE
Journal of Business, Economics & Governance
E ISSN 3124-792X
Volume 1 Nomor 2 Edisi Mei 2026 - Agustus 2026

Nilai F hitung sebesar 7,180 > 2,70 (F-tabel), Nilai signifikansi sebesar 0,009 < 0,05 menunjukkan bahwa Kepemimpinan Otoriter dan Tekanan Kerja secara simultan berpengaruh signifikan terhadap *Tindakan Cybercrime*. Dengan demikian hipotesis ketiga diterima.

Uji Koefisien Determinasi (R^2)

Tabel 15 Uji Koefisien Determinasi (R^2)

Model Summary[b]

					Change Statistics					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.208[a]	.043	.023	2.74454	.043	7.180	2	96	.009	2.330

a. Predictors: (Constant), X2, X1

b. Dependent Variable: Y

Sumber: Data Diolah Dari Hasil Penelitian, 2026

Nilai Adjusted R Square sebesar 4,3 menunjukkan bahwa sebesar 4,3% variasi Tindakan *Cybercrime* dapat dijelaskan oleh variabel Kepemimpinan Otoriter dan Tekanan Kerja. Sedangkan sisanya 95,7% dijelaskan oleh variabel lain yang tidak diteliti dalam penelitian ini.

PEMBAHASAN

Kepemimpinan Otoriter Berpengaruh Terhadap Tindakan *Cybercrime* Karyawan Bank Pemerintah di Indonesia

Berdasarkan hasil uji parsial (uji t), diperoleh nilai t hitung sebesar 0,600 dengan nilai signifikansi sebesar 0,550. Nilai signifikansi tersebut lebih besar dari 1,661 (t-tabel) (0,550 > 0,05), sehingga dapat disimpulkan bahwa Kepemimpinan Otoriter tidak berpengaruh signifikan terhadap *Tindakan Cybercrime*. Hal ini sesuai dengan penelitian (Song, 2023b) yang menyatakan bahwa tinggi atau rendahnya tingkat kepemimpinan otoriter yang diterapkan dalam organisasi tidak secara langsung mempengaruhi kecenderungan karyawan untuk melakukan tindakan *cybercrime*. Hal ini mengindikasikan bahwa tindakan *cybercrime* lebih dipengaruhi oleh faktor lain, seperti pengawasan sistem informasi, etika kerja, budaya organisasi, keamanan teknologi informasi, maupun karakteristik individu karyawan.

Kepemimpinan otoriter tidak berpengaruh signifikan terhadap tindakan *cybercrime* karena tinggi rendahnya tingkat kepemimpinan otoriter yang dirasakan karyawan tidak secara langsung meningkatkan ataupun menurunkan kecenderungan melakukan tindakan *cybercrime*

di lingkungan organisasi. Karena sektor perbankan merupakan industri yang memiliki tingkat regulasi dan pengawasan yang sangat tinggi. Aktivitas karyawan dibatasi oleh standar operasional, pengendalian internal, pemisahan tugas (*segregation of duties*), audit internal, pemantauan transaksi, serta pengelolaan hak akses yang ketat. Dengan adanya mekanisme tersebut, peluang untuk melakukan cybercrime menjadi lebih ditentukan oleh efektivitas sistem pengendalian daripada gaya kepemimpinan.

Tekanan Kerja Berpengaruh Terhadap Tindakan *Cybercrime* Karyawan Bank Pemerintah di Indonesia

Berdasarkan hasil uji parsial (uji t), diperoleh nilai t hitung sebesar 5,953 dengan nilai signifikansi sebesar 0,004. Nilai signifikansi tersebut lebih kecil dari 1,661 (t-tabel) (0,004 < 0,05), sehingga dapat disimpulkan bahwa Tekanan Kerja berpengaruh positif dan signifikan terhadap Tindakan *Cybercrime*. Hal ini sejalan dengan penelitian (Kwala and Agoyi, 2025) yang menyatakan bahwa proses semakin tinggi tekanan kerja yang dirasakan karyawan, maka semakin tinggi pula kecenderungan karyawan melakukan tindakan *cybercrime*. Sebaliknya, apabila tekanan kerja dapat diminimalkan, maka kecenderungan melakukan tindakan *cybercrime* akan menurun.

Tekanan Kerja berpengaruh positif dan signifikan terhadap Tindakan *Cybercrime* karena semakin tinggi tekanan kerja yang dialami karyawan, semakin besar kecenderungan munculnya perilaku yang mengarah pada penyalahgunaan sistem informasi, pelanggaran kebijakan keamanan informasi, atau tindakan cybercrime di lingkungan organisasi. Di sektor perbankan, tekanan kerja dapat berasal dari berbagai sumber, seperti target bisnis yang tinggi, tuntutan pelayanan yang cepat, volume transaksi yang besar, tenggat waktu yang ketat, pengawasan yang intensif, serta tanggung jawab menjaga keamanan dana dan data nasabah. Apabila tekanan tersebut berlangsung terus-menerus tanpa dukungan organisasi yang memadai, sebagian karyawan dapat mengambil jalan pintas (*shortcuts*) untuk menyelesaikan pekerjaan.

Kepemimpinan Otoriter dan Tekanan Kerja Berpengaruh Terhadap Tindakan *Cybercrime* Karyawan Bank Pemerintah di Indonesia

Berdasarkan hasil uji simultan (uji F), diperoleh nilai F hitung sebesar 7,180 > 2,70 (F-tabel), dengan tingkat signifikansi sebesar 0,009. Nilai signifikansi tersebut lebih kecil dari 0,05 (0,009 < 0,05), sehingga dapat disimpulkan bahwa Kepemimpinan Otoriter dan Tekanan Kerja secara simultan berpengaruh signifikan terhadap Tindakan *Cybercrime*. Hasil ini menunjukkan bahwa secara bersama-sama kedua variabel independen mampu menjelaskan

perubahan pada variabel Tindakan *Cybercrime*. Meskipun secara parsial Kepemimpinan Otoriter tidak berpengaruh signifikan, namun ketika dikombinasikan dengan Tekanan Kerja, keduanya memberikan kontribusi terhadap terbentuknya perilaku *cybercrime* di lingkungan organisasi.

KESIMPULAN

Berdasarkan hasil penelitian Kepemimpinan Otoriter tidak berpengaruh signifikan terhadap Tindakan *Cybercrime*, Tekanan Kerja berpengaruh positif dan signifikan terhadap Tindakan *Cybercrime* dan Kepemimpinan Otoriter dan Tekanan Kerja secara simultan berpengaruh signifikan terhadap Tindakan *Cybercrime*. Berdasarkan hasil penelitian yang telah dilakukan, maka penulis memberikan beberapa saran bagi pimpinan diharapkan mampu menciptakan lingkungan kerja yang lebih terbuka dan komunikatif sehingga karyawan dapat menyampaikan permasalahan pekerjaan yang dihadapi. Selain itu, peningkatan pengawasan terhadap penggunaan sistem informasi dan keamanan data organisasi perlu dilakukan untuk mencegah terjadinya penyalahgunaan teknologi informasi.

Temuan penelitian ini memberikan kontribusi teoretis dengan memperluas kajian perilaku organisasi dan keamanan informasi melalui pengintegrasian faktor kepemimpinan dan tekanan kerja sebagai determinan tindakan *cybercrime*. Penelitian ini menunjukkan bahwa perilaku *cybercrime* tidak hanya dipengaruhi oleh aspek teknis keamanan sistem, tetapi juga oleh kondisi psikologis dan lingkungan kerja yang dialami karyawan.

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan dalam menginterpretasikan hasil penelitian. Pertama, penelitian hanya menggunakan pendekatan kuantitatif melalui penyebaran kuesioner sehingga informasi yang diperoleh bergantung pada persepsi dan kejujuran responden dalam memberikan jawaban. Kedua, penelitian dilakukan pada satu organisasi atau wilayah tertentu sehingga hasil penelitian memiliki keterbatasan dalam hal generalisasi terhadap seluruh jenis organisasi atau sektor industry. Penelitian hanya mengkaji pengaruh kepemimpinan otoriter dan tekanan kerja terhadap tindakan *cybercrime*.

DAFTAR PUSTAKA

Blau and Stephens. (2025). Antecedents and Outcomes of Technology-Driven Workplace Deviant Behaviors. *Employee Responsibilities and Rights Journal*, 1–27.

Djailani, M. F. (2024). Mantan Pegawai Bank Jago Bobol 112 Rekening Nasabah Senilai Rp1,3

Miliar, Duitnya Buat Foya-foya. *Suara.Com*. https://www.suara.com/bisnis/2024/07/10/191750/mantan-pegawai-bank-jago-bobol-112-rekening-nasabah-senilai-rp13-miliar-duitnya-buat-foya-foya?utm_source=chatgpt.com

Gelman, Haywood, et al. (2023). Toward an Insider Threat Education Platform : A Theoretical Literature Review. *ArXiv Journal*, 1–6.

Ghozali, I. (2021). *Aplikasi Analisis Multivariate dengan Program IBM SPSS*.

Jones, L. A. (2024). Unveiling Human Factors : Aligning Facets of Cybersecurity Leadership , Insider Threats , and Arsonist Attributes to Reduce Cyber Risk. *SocioEconomic Challenges Journal*, *8*(2), 44–63.

Katto dan Pratama. (2023). Pengaruh Gaya Kepemimpinan, Pemberdayaan Sumber Daya Manusia, dan Lingkungan Kerja Terhadap Kepuasan Kerja Karyawan (Studi Empiris Pada Bank Mandiri Kantor Cabang Kota Magelang). *Jurnal Manajemen Bisnis Dan Terapan*, *1*(2), 86–96.

Kwala and Agoyi. (2025). The Influence of Cyberloafing on Workplace Outcomes: A Study Utilizing the Job Demands-Resources (JD-R) Theory. *SAGE Open*, *15*(1).

Loten, A. (2026). Hackers Recruit Unhappy Insiders to Bypass Data Security. *WSJ PRO*. https://www.wsj.com/articles/hackers-recruit-unhappy-insiders-to-bypass-data-security-a8ed6ec2?utm_source=chatgpt.com

Peng, Jian, et al. (2023). Participative leadership and employees' cyberloafing: A self-concept-based theory perspective. *Information & Management Journal*, *60*(8), 103878.

Rizqi and Swasti. (2025). Work Stress Mediates the Effect of Role Conflict on Cyberloafing Behaviour. *MSR Journal*, *4*(3), 54–60.

Robbins & Judge. (2022). *Organizational Behavior* (19th ed.). Pearson Education.

Shikonde and Nkongolo. (2025). A Proactive Insider Threat Management Framework Using Explainable Machine Learning. *ArXiv Journal*, 1–41.

Song, F. and L. (2023a). Exploring the Complex Relationships Between Factors That Affect Employee Cyberloafing Using a Novel Approach: Findings from Fuzzy-Set Qualitative Comparative Analysis. *Cyberpsychology, Behavior, and Social Networking Journal*, *26*(10), 1–7.

Song, F. and L. (2023b). Exploring the Complex Relationships Between Factors That Affect Employee Cyberloafing Using a Novel Approach: Findings from Fuzzy-Set Qualitative Comparative Analysis. *Cyberpsychology, Behavior, and Social Networking Journal*, *26*(10).

Zhang, Yajun, et al. (2022). Authoritarian Leadership and Cyberloafing : A Moderated Mediation Model of Emotional Exhaustion and Power Distance Orientation. *Front. Psychol. Journal*, 1–13. https://doi.org/10.3389/fpsyg.2022.1010845

Zhang et al. (2022). Kepemimpinan Otoriter berpengaruh Terhadap Cyberloafing Melalui Kelelahan Emosional. *Front. Psychol Journal*, *13*, 1010845.

Zhang, N. and W. (2022). Authoritarian Leadership and Cyberloafing : A Moderated Mediation Model of Emotional Exhaustion and Power Distance Orientation. *Front. Psychol Journal*, *13*, 1–13. https://doi.org/10.3389/fpsyg.2022.1010845

