https://doi.org/10.37817/ikraith-informatika.v8i2
P-ISSN 2580-4316
E-ISSN 2654-8054

Analisis Faktor-Faktor Keamanan Informasi Perusahaan Dalam Penerapan *Bring Your Own Device* (BYOD)

Rifda Aisy Nurillah[1], Agus Trihandoyo[2]
Universitas Siber Indonesia[1], Universitas Siber Indonesia [2]
E-mail: rifdaaisynurillah@gmail.com[1], agus.trihandoyo.fr@gmail.com[2]

ABSTRAK

Bring Your Own Device (BYOD) merupakan fenomena atau sebuah kegiatan dimana karyawan dalam suatu organisasi membawa perangkat komputer mereka sendiri untuk mengakses pekerjaan. Penerapan BYOD memiliki kelebihan dalam hal produktivitas, efektivitas, maupun fleksibilitas. Namun dalam pelaksanaannya, perusahaan menyadari bahwa BYOD dapat meningkatkan risiko atau ancaman terkait keamanan informasi. Penelitian ini menguji faktor keamanan informasi perusahaan yang dipengaruhi oleh *Mobile Device Management*, kebijakan keamanan informasi, budaya keamanan, dan pelatihan karyawan pada salah satu perusahaan perbankan di Indonesia. Analisis ini bertujuan untuk mengetahui faktor yang berpengaruh terhadap keamanan informasi perusahaan dalam menerapkan BYOD. Pengumpulan data dilakukan melalui kuesioner yang disebar kepada karyawan. Analisis data menggunakan metode *Partial Least Square* (PLS-SEM) dengan bantuan *software* SmartPLS. Hasil analisis menunjukkan bahwa terdapat pengaruh antara faktor-faktor yang diuji dalam model tersebut yang memperoleh nilai *R-Square* yaitu 0,666. Hasil tersebut dapat diartikan bahwa variabel bebas dalam penelitian ini, antara lain *Mobile Device Management,* kebijakan keamanan informasi, budaya keamanan, dan pelatihan karyawan mempengaruhi variabel terikat, yaitu keamanan informasi perusahaan sebesar 66,6%.

Kata kunci : ***Bring Your Own Device, Keamanan Informasi, Kebijakan Keamanan Informasi, Budaya Keamanan, Pelatihan Karyawan***

ABSTRACT

Bring Your Own Device (BYOD) is a phenomenon or an activity where employees in an organization bring their own computer devices to access work. The application of BYOD has advantages in terms of productivity, effectiveness, and flexibility. However, in practice, companies realize that BYOD can increase risks or threats related to information security. This research examines the company's information security factors that are influenced by Mobile Device Management, information security policy, security culture, and employee training at a banking company in Indonesia. This analysis aims to determine the factors that influence company information security when implementing BYOD. Data collection occurs through questionnaires distributed to employees. Data analysis using the method Partial Least Square (PLS-SEM) with the help of the software SmartPLS. The results of the analysis show that there is an influence between the factors tested in the model, which obtains a value of R-Square that is 0.666. These results can be interpreted as indicating that the independent variables in this study, including Mobile Device Management, information security policies, security culture, and employee training, affect the dependent variable, namely company information security by 66.6%.

Keyword : ***Bring Your Own Device, Information Security, Information Security Policy, Security Culture, Employee Training***

https://doi.org/10.37817/ikraith-informatika.v8i2
P-ISSN 2580-4316
E-ISSN 2654-8054

1. PENDAHULUAN

Teknologi informasi berkembang seiring berjalannya dengan pertumbuhan penggunaan internet. Terhitung pada Januari 2023, jumlah pengguna internet di Indonesia mencapai 212,9 juta pengguna, seperti pada Gambar 1.

Sumber: We Are Social

Gambar 1. Pertumbuhan Pengguna Internet di Indonesia

Berdasarkan laporan We Are Social, pertumbuhan pengguna internet di Indonesia meningkat sebanyak 3,85% dari tahun sebelumnya dengan 98,3% diantaranya diakses melalui telepon genggam (Rizaty, 2023). Perkembangan ini membawa perubahan pada segala aspek kehidupan, salah satunya pada cara kerja masyarakat yang ditandai dengan masuknya tren karyawan yang menggunakan perangkat sendiri saat bekerja. Fenomena membawa perangkat sendiri untuk mengakses pekerjaan biasa disebut dengan *Bring Your Own Device* (BYOD). Fenomena tersebut dikatakan mampu meningkatkan produktivitas, sebab ruang kerja karyawan tidak selalu hanya di kantor saja (Ratchford et al., 2022). Melainkan karyawan dapat tetap terhubung melalui jaringan perusahaan dimanapun dan kapanpun.

Fleksibilitas dan efektivitas yang diberikan pada konsep BYOD perlu diwaspadai, terutama ancaman terhadap keamanan informasi perusahaan. Dengan konsep BYOD, perusahaan mengizinkan karyawannya untuk memakai perangkat mereka sendiri untuk masuk ke jaringan perusahaan dan mengakses data internal perusahaan. Dengan segala kelebihan BYOD, terdapat kekurangan yang perlu dipertimbangkan perusahaan. Kebijakan BYOD dalam suatu organisasi biasanya dikaitkan dengan risiko privasi dan keamanan karena kurangnya kesadaran keamanan informasi pada karyawan (Mayayise, 2021). Pengguna yang awam dan sistem keamanan perangkat pribadi yang tidak mumpuni menjadi kekhawatiran perusahaan yang dapat mengundang *hacker* meretas dan mencuri data penting didalamnya. Oleh karena itu, pengelolaan keamanan informasi diperlukan untuk menjaga kerahasiaan, ketersediaan, dan integritas sumber daya perusahaan (Nurul dkk., 2022).

Di dalam penelitian sebelumnya tentang pengembangan model manajemen risiko BYOD menghasilkan model berdasarkan faktor-faktor keamanan yang telah diuji pada sebuah organisasi (Veljkovic & Budree, 2019). Penelitian ini akan fokus pada pengujian beberapa faktor pada penelitian tersebut, yaitu *Mobile Device Management*, kebijakan keamanan informasi, budaya keamanan, dan pelatihan karyawan terhadap keamanan informasi perusahaan pada sebuah perusahaan perbankan di Indonesia.

2. LANDASAN TEORI

2.1 *Bring Your Own Device*

Bring Your Own Device (BYOD) merupakan sebuah kegiatan dimana karyawan dalam organisasi membawa perangkat pribadi, seperti *smartphone*, *tablet*, dan laptop ke tempat kerja untuk mengakses data dan pekerjaan mereka melalui jaringan perusahaan (Idris, 2019).

Perusahaan/organisasi menyadari bahwa kebijakan ini dapat meningkatkan produktivitas pekerja dan mengurangi

P-ISSN 2580-4316
E-ISSN 2654-8054

biaya operasional (Ratchford et al., 2022). Namun, adanya kebijakan BYOD ini meningkatkan risiko atau ancaman terkait keamanan data/informasi perusahaan, sehingga perlu diperhatikan terutama pada keamanan perangkat.

2.2 *Structural Equation Modeling*

Metode *Structural Equation Modeling* (SEM) merupakan salah satu metode untuk menganalisis model persamaan jalur. Dalam metode SEM, terdapat 2 model analisis yang umum digunakan, yaitu *Covariance-Based Structural Equation Modeling* (CB-SEM) dan *Partial Least Squares Path Modeling* (PLS-SEM) (Hamid & Anwar, 2019:2). Penggunaan PLS-SEM bertujuan untuk menguji hubungan prediktif antar konstruk berdasarkan pengaruhnya.

Analisis PLS-SEM membanding-kan beberapa variabel dependen dan independen sebagai pendekatan statistik multivariat. Masalah dengan spesifikasi data yang muncul dalam regresi berganda, seperti ukuran sampel yang terbatas, data kosong/hilang, dan adanya multikolinearitas, dapat diselesaikan dengan menggunakan PLS. (Hamid & Anwar, 2019:15).

2.3 *Mobile Device Management*

Mobile Device Management (MDM) merupakan sebuah alat yang digunakan untuk mengontrol, memantau, dan melindungi perangkat seluler. MDM membantu perusahaan dalam mengelola jaringan komputasi dan lingkungan komunikasi dengan tetap menjaga keamanan data/informasi. Perusahaan menggunakan MDM agar dapat mengontrol perangkat dengan baik tanpa mengurangi kenyamanan penggunanya (Mega Puspita & Hasanudin, 2022).

2.4 Kebijakan Keamanan Informasi

Kebijakan keamanan informasi adalah serangkaian peraturan yang dibuat untuk menjaga keamanan informasi dengan tujuan memastikan bahwa semuanya aman. Perusahaan menerapkan kebijakan sesuai sektor dan lembaga yang menaunginya. Kurangnya kebijakan seringkali membuat suatu perusahaan/ organisasi terpapar berbagai risiko BYOD. Oleh karena itu, pentingnya menetapkan kebijakan yang efektif untuk menghindari potensi pelanggaran keamanan. Sebab, perusahaan yang mengizinkan karyawannya menggunakan perangkat mereka sendiri dengan kurangnya kebijakan yang sesuai, tanpa disadari akan membuat organisasi terpapar sejumlah risiko BYOD yang besar (Veljkovic & Budree, 2019).

2.5 Budaya Keamanan

Budaya keamanan diidentifikasi-kan dengan ciri utama yaitu, aspek-aspek seperti pekerja yang berpengetahuan, menyadari, dan menerapkan perilaku teliti dan peduli untuk mematuhi kebijakan yang disepakati organisasi. Budaya keamanan informasi yang ideal dapat membantu meminimalisir ancaman keamanan informasi, maka diharapkan juga mengurangi adanya pelanggaran data atau insiden dalam organisasi (da Veiga et al., 2020).

2.6 Pelatihan Karyawan

Bagi suatu perusahaan, karyawan merupakan aset penting untuk mengoperasikan bisnis di dalamnya. Dalam konsep BYOD, perusahaan secara tidak langsung kehilangan kendali atas keamanan perangkat mereka, karyawan memiliki peran yang signifikan dalam menjaga keamanan organisasi secara umum (Veljkovic & Budree, 2019). Namun, karyawan dianggap sebagai mata rantai keamanan yang paling rapuh saat menerapkan strategi BYOD. Sehingga, dibutuhkan manajemen sumber daya yang baik untuk mengelola karyawan agar tidak berakibat fatal bagi perusahaan. Salah satunya dengan mengadakan pelatihan karyawan.

https://doi.org/10.37817/ikraith-informatika.v8i2
P-ISSN 2580-4316
E-ISSN 2654-8054

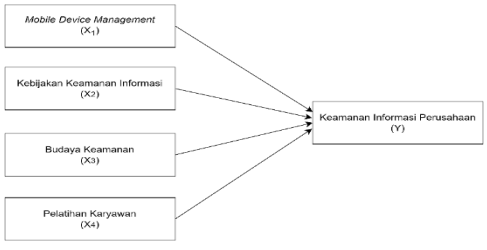
2.7 Keamanan Informasi Perusahaan

Informasi/data adalah aset vital yang harus dilindungi perusahaan. Keamanan informasi dapat didefinisikan sebagai upaya untuk melindungi aset informasi dari bahaya yang mungkin terjadi. Terdapat tiga tujuan utama untuk mencapai keamanan informasi, yaitu kerahasiaan (*Confidentiality*), integritas (*Integrity*), dan ketersediaan (*Availability*) (Nurul dkk., 2022). Kerahasiaan merupakan aspek yang memastikan informasi hanya dapat diakses oleh pihak yang berwenang. Dan integritas merupakan aspek yang menjamin bahwa data tidak berubah tanpa seizin pihak yang berwenang sehingga terjaga keakuratan dan keutuhannya. Sedangkan, ketersediaan merupakan aspek yang memberi jaminan atas ketersediaan data saat dibutuhkan.

Mengingat pentingnya keamanan informasi perusahaan, penerapan BYOD perlu dipersiapkan dengan baik. Pasalnya tren BYOD menarik pelaku ancaman untuk melakukan serangan siber yang mengakses data sensitif perusahaan. Namun pada saat yang sama, tren BYOD dapat meningkatkan produktivitas karyawan dan operasional bisnisnya.

2.8 Kerangka Konseptual

Berdasarkan kajian teori yang telah dibahas, maka dibuat kerangka pikir yang dinyatakan dalam bentuk diagram alur penelitian, seperti pada Gambar 2.



Gambar 2. Kerangka Konseptual

Penelitian ini memiliki 4 variabel bebas yaitu, *Mobile Device Management* (X_1), Kebijakan Keamanan Informasi (X_2), Budaya Keamanan (X_3), dan Pelatihan Karyawan (X_4), yang memiliki pengaruh terhadap Keamanan Informasi Perusahaan (Y). Dengan rumusan hipotesis sebagai berikut:

a. H1: *Mobile Device Management* berpengaruh terhadap keamanan informasi perusahaan.
b. H2: Kebijakan keamanan informasi berpengaruh terhadap keamanan informasi perusahaan.
c. H3: Budaya keamanan berpengaruh terhadap keamanan informasi perusahaan.
d. H4: Pelatihan karyawan berpengaruh terhadap keamanan informasi perusahaan.

3. METODOLOGI

3.1 Jenis dan Sumber Data Peneltian

Penelitian ini menggunakan pendekatan kuantitatif. Menurut Hardani (2020:248), penelitian kuantitatif merupakan jenis penelitian yang analisisnya berfokus pada data berupa angka yang diolah dengan statistik. Data kuantitatif merupakan data yang menunjukkan kuantitas berbentuk angka agar dapat ditentukan besarannya (Hardani dkk, 2020:246). Adapun sumber data yang digunakan dalam penelitian ini, yaitu data primer yang berasal dari pengisian kuesioner.

3.2 Fokus dan Objek Penelitian

Penelitian ini berfokus pada pengujian faktor-faktor yang memiliki pengaruh terhadap keamanan informasi perusahaan pada penerapan BYOD. Dalam pengujian tersebut, penelitian dilakukan pada perusahaan di sektor perbankan. Berkaitan dengan keamanan informasi sebuah perusahaan, maka akan ada peraturan atau kebijakan untuk meminimalisir risiko. Oleh karena itu, nama perusahaan akan disamarkan menjadi Bank XYZ. Bank XYZ merupakan perbankan syariah di

P-ISSN 2580-4316
E-ISSN 2654-8054

Indonesia yang sudah menerapkan kebijakan BYOD di perusahaannya.

3.3 Penentuan Populasi dan Sampel

Populasi merupakan keseluruhan objek dalam penelitian, sedangkan sampel hanya sebagian dari populasi. Pemilihan sampel perlu dilakukan dengan teknik yang tepat agar sampel dapat mencerminkan karakteristik dari populasi (Fauzy, 2019). Penentuan sampel menggunakan teknik *non-probability sampling*, dimana sampel diambil tidak secara acak. Berdasarkan tujuan dan objek yang digunakan, pengambilan sampel dilakukan dengan cara *purposive sampling*.

Purposive sampling merupakan teknik pengambilan sampel yang dilakukan dengan ketentuan tertentu. Ketentuan dalam hal ini keterbatasan perizinan yang dimiliki peneliti dalam mengumpulkan data pada perusahaan Bank XYZ. Sehingga populasi yang diteliti hanya para karyawan di Bank XYZ pada divisi Kepatuhan, Risiko & Hukum yang berjumlah 36 orang.

Ukuran sampel harus mewakili populasi. Menurut Slovin, minimal sampel yang diambil menggunakan rumus berikut (Fauzy, 2019).

$$n = \frac{N}{1 + N.e^2} \quad (1)$$

Keterangan:
n = ukuran sampel,
N = ukuran populasi,
e = persentase toleransi kesalahan (5%)

$$n = \frac{N}{1 + N.e^2}$$
$$n = \frac{36}{1 + (36)(0.05)^2}$$
$$n = \frac{36}{1 + 0{,}09}$$
$$n = 33{,}02$$

Ukuran sampel yang diperoleh dari perhitungan Rumus Slovin adalah 33,02, dibulatkan menjadi 33. Dengan demikian, jumlah sampel yang harus diambil dalam penelitian ini minimal 33 karyawan/responden.

3.4 Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini dilakukan melalui kuesioner. Kuesioner adalah metode pengumpulan data dengan mengajukan pertanyaan atau pernyataan kepada orang yang disurvei untuk mendapatkan tanggapan (Riyanto dkk, 2020:29). Dalam penelitian ini, kuesioner disebarkan secara *online* dalam bentuk Google Forms kepada karyawan Bank XYZ.

3.5 Definisi Operasional

Menurut Hardani (2020:303) variabel penelitian disebut juga sebagai karakteristik atau sifat dari objek yang diteliti. Penelitian ini menggunakan dua variabel, yaitu variabel bebas dan terikat.

Variabel Bebas

Variabel bebas (*Independent Variable*) merupakan variabel yang menjadi penyebab atau mempengaruhi variabel terikat (Riyanto dkk, 2020:22). Berikut rincian indikator pengukuran dalam variabel bebas ditampilkan pada Tabel 1 (Veljkovic & Budree, 2019) dan (Dalla, 2021).

Tabel 1. Variabel Bebas

Variabel Bebas	***Indikator***	***Rincian Indikator***
Mobile Device Management (X1)	X1.1	Pengetahuan tentang kebijakan MDM di perusahaan.
	X1.2	Penerapan kebijakan MDM di perusahaan.
Kebijakan Keamanan Informasi (X2)	X2.1	Pengetahuan tentang kebijakan keamanan Informasi di perusahaan.
	X2.2	Penerapan kebijakan keamanan Informasi di perusahaan.
	X2.3	Efektivitas kebijakan keamanan informasi

P-ISSN 2580-4316
E-ISSN 2654-8054

Variabel Bebas	*Indikator*	*Rincian Indikator*
		dalam melindungi informasi perusahaan.
	X2.4	Kesadaran karyawan akan prioritas keamanan informasi perusahaan.
Budaya Keamanan (X3)	X3.1	Pelaporan insiden/ pelanggaran data oleh karyawan.
	X3.2	Kemampuan karyawan dalam menangani insiden/pelanggaran data.
	X3.3	Kesadaran karyawan terhadap ancaman keamanan saat menggunakan perangkat pribadi.
	X3.4	Kekhawatiran karyawan terhadap potensi risiko keamanan saat menggunakan perangkat pribadi.
Pelatihan Karyawan (X4)	X4.1	Penyediaan pelatihan karyawan oleh perusahaan.
	X4.2	Pelaksanaan pelatihan karyawan oleh perusahaan secara teratur.
	X4.3	Penerimaan pelatihan karyawan terkait keamanan informasi
	X4.4	Pengetahuan tentang penerapan keamanan informasi

Variabel Terikat

Variabel terikat (*Dependent Variable*) merupakan variabel yang dipengaruhi atau yang menjadi akibat dari variabel bebas (Riyanto dkk, 2020:22). Berikut rincian indikator pengukuran dalam variabel terikat ditampilkan pada Tabel 2 (Veljkovic & Budree, 2019) dan (Dalla, 2021).

Tabel 2. Variabel Terikat

Variabel Terikat	*Indikator*	*Rincian Indikator*
Keamanan Informasi Perusahaan (Y)	Y1	Peningkatan produktivitas penggunaan perangkat pribadi untuk pekerjaan.
	Y2	Kemudahan penggunaan perangkat pribadi untuk pekerjaan.
	Y3	Kemudahan proses pengintegrasian perangkat pribadi untuk pekerjaan.
	Y4	Kepuasan karyawan terhadap tingkat keamanan informasi perusahaan.
	Y5	Perusahaan mengalami serangan siber/ pelanggaran data.
	Y6	Jaringan perusahaan mengalami gangguan akibat serangan siber/ pelanggaran data.

3.6 Analisis Awal

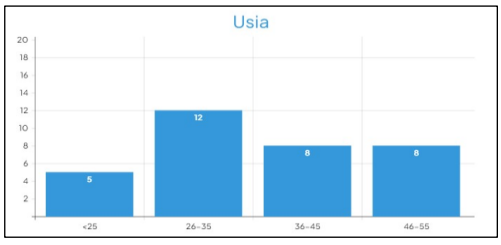
Pada tahap ini peneliti melakukan wawancara kepada beberapa pihak. Wawancara pertama dilakukan dengan Direktur Divisi Kepatuhan, Risiko dan Hukum Bank XYZ. Berdasarkan hasil wawancara tersebut, diketahui objek yang diteliti sudah menerapkan kebijakan BYOD. Wawancara kedua dilakukan di divisi *Information Security* pada sebuah perusahaan perbankan terhadap 3 orang pakar/ahli. Wawancara kedua dilakukan untuk me-*review* pertanyaan yang akan diajukan.

3.6 Teknik Analisis Data

Analisis data dilakukan dengan metode analisis PLS-SEM menggunakan *tools* SmartPLS versi 3.2.8. Teknik analisis yang dilakukan peneliti dimulai dari model pengukuran, uji reliabilitas, dan model struktural.

4. HASIL DAN PEMBAHASAN

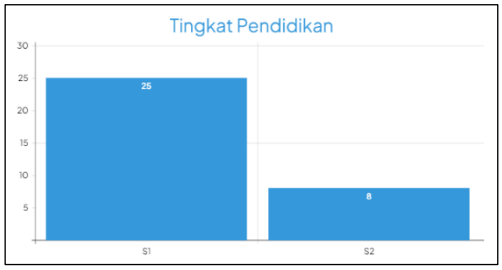
4.1 Profil Responden



Gambar 3. Profil Responden Berdasarkan Usia

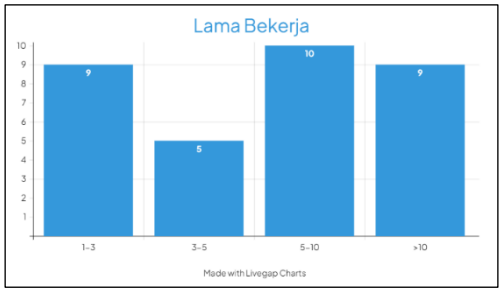
P-ISSN 2580-4316
E-ISSN 2654-8054

Berdasarkan Gambar 3 di atas, menunjukkan bahwa sebagian besar responden berada pada kelompok usia 26 tahun hingga 35 tahun berjumlah 12 orang (36,4%), dan pada kelompok usia 36 tahun hingga 45 tahun berjumlah 8 orang (24,2%), sama dengan kelompok usia 46 tahun hingga 56 tahun, yaitu sebanyak 8 orang (24,2%), sementara sisanya pada kelompok usia dibawah 25 tahun berjumlah 5 orang (15,2%).



Gambar 4. Profil Responden Berdasarkan Tingkat Pendidikan

Berdasarkan Gambar 4 di atas, menunjukkan bahwa mayoritas responden berpendidikan S1 (Strata-1) berjumlah 25 orang (75,8%), sementara sisanya berpendidikan S2 (Strata-2) berjumlah 8 orang (24,2%).



Gambar 5. Profil Responden Berdasarkan Lama Bekerja

Berdasarkan Gambar 5 di atas, menunjukkan bahwa jumlah responden dengan rentang waktu bekerja selama 5 sampai 10 tahun berjumlah 10 orang (30,3%), dan responden yang bekerja selama 1 sampai dengan 3 tahun sebanyak 9 orang (27,3%), sama halnya dengan responden yang bekerja selama lebih dari 10 tahun, yaitu sebanyak 9 orang (27,3%), sementara sisanya untuk responden yang bekerja selama 3 sampai 5 tahun berjumlah 5 orang (15,1%).

4.2 Hasil Analisis Data

Analisis data yang telah terkumpul pada penelitian ini dilakukan dengan metode *Partial Least Square* (PLS-SEM) menggunakan *software* SmartPLS versi 3.2.8. seperti pada Gambar 6.

Gambar 6. Path Model

Model Pengukuran (*Outer Model*)
Uji Validitas Konvergen

Tabel 3. Uji Validitas Konvergen

Variabel	Indikator	*Loading*	AVE
Mobile Device Management **(X1)**	X1.1	0.951	0.835
	X1.2	0.875	
Kebijakan Keamanan Informasi **(X2)**	X2.1	0.832	0.623
	X2.2	0.599	
	X2.3	0.841	
	X2.4	0.855	
Budaya Keamanan **(X3)**	X3.1	0.702	0.583
	X3.2	0.862	
	X3.3	0.780	
	X3.4	0.699	
Pelatihan Karyawan **(X4)**	X4.1	0.864	0.723
	X4.2	0.777	
	X4.3	0.879	
	X4.4	0.877	
Keamanan Informasi Perusahaan **(Y)**	Y1	0.791	0.653
	Y2	0.850	
	Y3	0.840	
	Y4	0.826	
	Y5	0.704	
	Y6	0.827	

https://doi.org/10.37817/ikraith-informatika.v8i2
P-ISSN 2580-4316
E-ISSN 2654-8054

Berdasarkan Tabel 3 terlihat bahwa setiap item pernyataan pada masing-masing variabel telah memenuhi syarat uji validitas konvergen, yaitu memiliki nilai *loading* dan AVE melebihi 0,5 yang berarti seluruh indikator dapat dikatakan valid.

Uji Validitas Diskriminan

Tabel 4. Nilai Korelasi Antar Variabel

Variabel	X1	X2	X3	X4	Y
X1	**0.914**				
X2	0.371	**0.789**			
X3	0.482	0.402	**0.764**		
X4	0.511	0.314	0.624	**0.850**	
Y	0.702	0.614	0.375	0.498	**0.808**

Berdasarkan Tabel 4 dapat diamati bahwa nilai korelasi antar setiap variabel dengan dirinya sendiri lebih tinggi dibandingkan dengan nilai korelasi antara variabel dengan variabel lainnya.

Tabel 5. Nilai *Cross Loading*

	X1	X2	X3	X4	Y
X1.1	**0.951**	0.457	0.509	0.568	0.752
X1.2	**0.875**	0.162	0.344	0.319	0.482
X2.1	0.346	**0.832**	0.417	0.362	0.41
X2.2	0.208	**0.599**	0.248	0.279	0.266
X2.3	0.326	**0.841**	0.255	0.182	0.588
X2.4	0.283	**0.855**	0.367	0.239	0.572
X3.1	0.305	0.487	**0.702**	0.299	0.349
X3.2	0.511	0.232	**0.862**	0.689	0.312
X3.3	0.351	0.282	**0.780**	0.475	0.256
X3.4	0.250	0.068	**0.699**	0.468	0.131
X4.1	0.482	0.404	0.535	**0.864**	0.491
X4.2	0.325	0.141	0.428	**0.777**	0.286
X4.3	0.411	0.168	0.528	**0.879**	0.368
X4.4	0.479	0.284	0.601	**0.877**	0.489
Y1	0.594	0.526	0.376	0.571	**0.791**
Y2	0.576	0.609	0.399	0.351	**0.850**
Y3	0.616	0.570	0.422	0.445	**0.840**
Y4	0.554	0.570	0.244	0.434	**0.826**
Y5	0.471	0.276	0.147	0.163	**0.704**
Y6	0.575	0.341	0.164	0.370	**0.827**

Berdasarkan Tabel 5 terlihat bahwa setiap indikator memiliki nilai *loading* lebih tinggi pada setiap variabel yang diukur dibandingkan dengan indikator pada variabel lainnya. Sehingga semua konstruk terbukti memiliki validitas diskriminan yang tinggi.

Uji Reliabilitas

Tabel 6. Uji Reliabilitas

Variabel	*Composite Reliability*	*Cronbach's Alpha*
X1	0.910	0.811
X2	0.866	0.800
X3	0.847	0.776
X4	0.912	0.875
Y	0.918	0.894

Berdasarkan Tabel 6 terlihat bahwa setiap variabel telah memenuhi syarat uji reliabilitas, yaitu memiliki nilai *Composite Reliability* dan *Cronbach's Alpha* melebihi 0,7 yang berarti seluruh variabel dapat dianggap reliabel.

Model Struktural (Inner Model)
R-Square

Tabel 7. Nilai *R-Square*

Variabel	R Square
Keamanan Informasi Perusahaan **(Y)**	0.666

Berdasarkan Tabel 7 diperoleh nilai *r-square* untuk variabel Keamanan Informasi Perusahaan (Y) sebesar 0,666, yang berarti bahwa variabel bebas mempengaruhi variabel terikatnya sebesar 66,6%, sedangkan 33,4% sisanya dipengaruhi oleh variabel lain.

Uji Signifikansi

Tabel 8. Uji Signifikansi

Path	*Path Coefficient*	T Statistik
X1 ➔ Y	0.524	3.814
X2 ➔ Y	0.426	2.680
X3 ➔ Y	-0.179	1.026
X4 ➔ Y	0.209	1.215

Berdasarkan Tabel 8 diketahui masing-masing hipotesis melihat hasil

P-ISSN 2580-4316
E-ISSN 2654-8054

Path Coefficient untuk mengindikasikan nilai pengaruh variabel bebas terhadap variabel terikat, sedangkan T Statistik menunjukkan pengaruh signifikansinya apabila nilai T Statistik lebih besar dari nilai T Tabel, yaitu 1,96. Pengaruh X1 terhadap Y dengan nilai *Path Coefficient* sebesar 0,524 dan nilai T statistik sebesar 3,814, mengindikasikan bahwa *Mobile Device Management* memiliki pengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan. Dan pengaruh X2 terhadap Y dengan nilai *Path Coefficient* sebesar 0,426 dan nilai T statistik sebesar 2,680, menunjukkan bahwa Kebijakan Keamanan Informasi memiliki pengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan. Sedangkan, pengaruh X3 terhadap Y dengan nilai *Path Coefficient* sebesar -0,179 dan nilai T statistik sebesar 1,026, menunjukkan Budaya Keamanan tidak memiliki pengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan. Sementara pengaruh X4 terhadap Y dengan nilai *Path Coefficient* sebesar 0,209 dan nilai T statistik sebesar 1,215, menunjukkan Pelatihan Karyawan memiliki pengaruh positif namun tidak signifikan terhadap Keamanan Informasi Perusahaan.

4.3 Pembahasan

Hipotesis pertama membuktikan *Mobile Device Management* berpengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan. Hal ini menunjukkan penerapan MDM dalam mengelola risiko BYOD pada perangkat pribadi karyawan mempengaruhi tingkat keamanan data/ informasi di dalamnya. Hasil ini mendukung penelitian Veljkovic dan Budree (2019), yang menyatakan penerapan solusi tersebut dapat menyelesaikan bahaya/ancaman teknologi yang teridentifkasi serta memperkuat keamanan informasi perusahaan.

Hipotesis kedua membuktikan Kebijakan Keamanan Informasi memiliki pengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan. Hal ini mengindikasikan penerapan kebijakan keamanan informasi dalam pelaksanaan BYOD pada perusahaan mempengaruhi tingkat keamanan informasinya. Hasil ini konsisten dengan penelitian yang dilakukan oleh Dalla (2021).

Hipotesis ketiga menunjukkan Budaya Keamanan tidak berpengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan. Hal ini mengindikasikan adanya budaya keamanan pada pelaksanaan BYOD tidak secara langsung mempengaruhi tingkat keamanan informasinya. Namun, jika dilihat dari pernyataan yang diajukan, ada beberapa hal tidak relevan dengan budaya pada divisi tersebut. Seperti halnya melaporkan ataupun menangani insiden/masalah keamanan, hal itu sesuai dengan karyawan di bagian IT (*Information Technology*) tetapi tidak pada divisi pada penelitian ini. Hasil ini juga sejalan dengan penelitian Dalla (2021), yang menunjukkan budaya keamanan berpengaruh negatif atau berkontribusi terhadap penurunan keamanan informasi perusahaan.

Hipotesis keempat menunjukkan bahwa Pelatihan Karyawan tidak berpengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan. Hal ini disebabkan karena pelatihan yang didapatkan karyawan pada divisi kepatuhan, risiko, dan hukum pada penelitian ini bukan terkait dengan pentingnya mengetahui dan menerapkan keamanan informasi. Pasalnya, setiap divisi pasti mengadakan pelatihan secara teratur, namun tujuan pelatihan yang diberikan berbeda-beda sesuai kebutuhannya. Hasil ini tidak konsisten dengan penelitian Dalla (2021), yang menyatakan bahwa pelatihan karyawan berpengaruh positif dan signifikan terhadap keamanan informasi perusahaan dalam penerapan BYOD.

P-ISSN 2580-4316
E-ISSN 2654-8054

5. KESIMPULAN

Berdasarkan hasil analisis data yang sudah dilakukan pada penelitian ini, dapat disimpulkan bahwa:

a. *Mobile Device Management* dan Kebijakan Keamanan Informasi memiliki pengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan.
b. Budaya Keamanan dan Pelatihan Karyawan tidak berpengaruh positif dan signifikan terhadap Keamanan Informasi Perusahaan.
c. Keamanan Informasi Perusahaan memiliki nilai pengaruh sebesar 66,6% yang dipengaruhi oleh variabel *Mobile Device Management*, Kebijakan Keamanan Informasi, Budaya Keamanan, dan Pelatihan Karyawan.

Disarankan kepada Bank XYZ maupun perusahaan lainnya agar dapat mempertimbangkan faktor tersebut untuk meningkatkan keamanan informasi dalam menerapkan kebijakan BYOD, terlebih dengan memperhatikan budaya dan pelatihan yang cocok untuk karyawannya yang diharapkan dapat mencegah risiko keamanan informasi perusahaan.

DAFTAR PUSTAKA

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture Perspectives from academia and industry. *Computers and Security*, *92*.

Dalla, G. M. (2021). *A Model Of Byod Integration To Increase Corporate Information Security In Banks: Case Of Equity Bank Kenya*. KCA University.

Fauzy, A. (2019). *Metode Sampling* (2nd ed.). Universitas Terbuka.

Hamid, R. S., & Anwar, S. M. (2019). *Structural Equation Modeling (SEM) Berbasis Varian: Konsep Dasar dan Aplikasi dengan Program SmartPLS 3.2.8 dalam Riset Bisnis* (Abiratno, S. Nurdiyanti, & A. D. Raksanagara, Eds). PT Inkubator Penulis Indonesia.

Hardani, Andriani, H., Ustiawaty, J., Utami, E. F., Auliya, N. H., Fardani, R. A., Sukmana, D. J., & Istiqomah, R. R. (2020). *METODE PENELITIAN Kualitatif & Kuantitatif* (H. Abadi, Ed.). CV. Pustaka Ilmu.

Idris, M. (2019). Pemilihan Solusi Penerapan Bring Your Own Device (BYOD) Berdasarkan Kontrol Keamanannya. *Jurnal Ilmiah MATRIK*, *21*(3).

Mayayise, T. (2021). Extending unified theory of acceptance and use of technology with ISO/IEC 27001 security standard to investigate factors influencing Bring Your Own Device adoption in South Africa. *South African Journal of Information Management Affiliation*, 1–9.

Mega Puspita, Y., & Hasanudin, M. (2022). Mobile Device Management for the Use of Bring Your Own Device (BYOD) as Company Data Security during the Covid-19 Pandemic. *International Journal of Information System & Technology Akreditasi*, *6*(158), 528–536.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review Sim). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5).

Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: a systematic literature review. *Information Security Journal*, *31*(3), 253–273.

Riyanto, S., & Hatmawan, A. A. (2020). *Metode Riset Penelitian Kuantitatif Penelitian di Bidang Manajemen, Teknik, Pendidikan dan Eksperimen* (G. D. Ayu, Ed.). CV BUDI UTAMA.

Rizaty, M. A. (2023, February 3). Pengguna Internet di Indonesia Sentuh 212 Juta pada 2023. *DataIndonesia.Id*.

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model: Case Study From a South African Organisation. *The Electronic Journal Information Systems Evaluation*, *22*(1), 1–14. www.ejise.com