e-ISSN: 2963-0185, p-ISSN: 2963-0142
DOI: https://doi.org//10-38035/jmpd.v1.i2
Received: 14/Maret/2023, Revised: 03/April/2023, Publish: 29/April/2023

Siber Nusantara Publisher
Jurnal Manajemen dan Pemasaran Digital (JMPD)
+62 811 7404 445 http://siberpublisher.org siberpublisher.info@gmail.com Casa Amira Prive Jl. H. Risin No. 64D Pondok Jagung Timur, Serpong Utara, Tangerang Selatan, Indonesia.

Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder

Abdul Halim Harahap[1], Claresta Difa Andani[2], Angelia Christie[3], Divtyajeng Nurhaliza[4], Ahmad Fauzi[5]

[1] Fakultas Ekonomi, Universitas Bhayangkara Jakarta Raya, 202110315016@mhs.ubharajaya.ac.id
[2] Fakultas Ekonomi, Universitas Bhayangkara Jakarta Raya, 202110315051@mhs.ubharajaya.ac.id
[3] Fakultas Ekonomi, Universitas Bhayangkara Jakarta Raya, 202110315099@mhs.ubharajaya.ac.id
[4] Fakultas Ekonomi, Universitas Bhayangkara Jakarta Raya, 202110315003@mhs.ubharajaya.ac.id
[5] Fakultas Ekonomi, Universitas Bhayangkara Jakarta Raya, Achmad.fauzi@dsn.ubharajaya.ac.id

Corresponding Author: Abdul Halim Harahap[1]

Abstrak: Dalam keberlangsungan suatu organisasi atau perusahaan adalah hal yang penting untuk melindungi aset-aset terkait organisasi atau perusahaan yang dijalankan. Aset-aset penting perusahaan dan organisasi mencakupi hal-hal yang menjamin keberlangsungan suatu organisasi dan perusahaan itu sendiri. Informasi dan data terkait organisasi atau perusahaan merupakan hal yang paling penting untuk dilindungi keamanannya. Dalam melindungi keamanan informasi dan data, dalam tulisan ini membahas Spesifik indikator-indikator keamanan organisasi atau perusahaan. Indikator keamanan ini dikenal dengan "CIA Triad" yaitu Confidentiality (Kerahasiaan), Integrity (Integritas), Availability (Ketersediaan). Dalam penelitian ini membahas CIA TRIAD dalam melindungi keamanan informasi dan data dalam suatu sistem yang diterapkan. Ketiga faktor ini saling berkaitan dan saling menjaga ikatan satu sama lain, dengan kata lain jika salah satu faktor tersebut dihilangkan Keamanan informasi dan data akan sangat beresiko. Maka dari itu keterkaitan CIA Triad sangatlah berperan penting dan memiliki pengaruh.

Kata Kunci: Kerahasiaan (Confidentiality), integritas (Integrity), dan ketersediaan (Availability). Keamanan sistem informasi dan data, CIA Triad.

PENDAHULUAN

Berdasarkan perkembangan zaman, teknologi adalah salah satu kunci manusia untuk melakukan segala hal untuk dapat memudahkan pekerjaan mereka. Dalam era digital yang terus berkembang, perlindungan informasi dan keamanan data telah menjadi aspek yang sangat penting dalam kehidupan sehari-hari Teknologi banyak digunakan dalam berbagai hal

dalam kehidupan manusia. Sistem computer pada saat ini menjadi salah satu teknologi yang mengambil peran penting terhadap suatu perkembangan. Semua hal yang berbasis computer atau yang dilakukan dengan komputerisasi akan sangat mudah di akses jika tidak memiliki pedoman atau landasan keamanan sistem informasi. Hal tersebut tentunya dapat dimanfaatkan oleh pelaku tindak kejahatan dan menjadi sebuah ancaman bagi pengguna atau user sistem informasi teknologi. Hal ini tentunya dapat menjadi suatu masalah besar karena keamanan dan kerahasiaan data merupakan salah satu faktor penting yang harus diperhatikan dalam komunikasi terutama dengan kemajuan dan perkembangan teknologi pada masa kini. Pesatnya perkembangan teknologi memberikan banyak dampak positif bagi masyarakat seperti kemudahan memperoleh informasi, pertukaran data dan pesan penyebaran informasi, pengiriman pesan, dan sebagainya.

Pengembang suatu bisnis atau sebuah developer yang menggunakan teknologi digital tentunya pasti menyadari pentingnya menjaga keamanan data para penggunanya demi menunjang segala bisnis yang mereka jalani. Ancaman nyata yang menyerang sistem informasi seperti kebocoran sebuah data, kredensial (kompromi akun), phishing, serangan berbasis web, serangan malware, cracking (pembajakan), carding (transaksi ilegal) dan sebagainya.

Jenis-jenis kejahatan yang telah disebutkan tentunya pasti bisa diantisipasi atau dihindari. Suatu organisasi tentunya memiliki kewajiban penuh untuk menjaga data-data pengguna demi menjaga kepercayaan pelanggan dan juga sebagai pemenuh kebutuhan terhadap segala aturan. Cyber Crime memiliki tujuan mengganggu kedaulatan sebuah organisasi dan mengambil keuntungan sendiri dengan membenarkan segala cara dan mengeksploitasi data demi mendapatkan keuntungan yang mereka inginkan.

Berdasarkan pemaparan di atas, dapat diketahui bahwa sistem informasi dan data memiliki resiko terhadap ancaman Cyber Crime yang semakin marak terjadi. Untuk menghadapi tantangan tersebut riset ini ditujukan untuk mengetahui dan menganalisis apakah konsep dari Cyber Cerurity yaitu CIA Triad dimana mengacu terhadap pemaparan dalam memastikan kerahasiaan (Confidentiality), integritas (Integrity) dan ketersediaan (Availability) akan menjadi model yang perannya dinilai memiliki efektifitas terhadap keamanan sistem informasi dan data.

Berdasarkan latar belakang di atas maka permasalahan yang didapatkan sebagai berikut:

1. Dengan cara apa *Cyber Crime* dapat dicegah?
2. Apakah konsep CIA triad penting dalam menjaga keamanan data?
3. Apakah konsep CIA triad dapat digunakan sebagai pedoman dan kerangka kerja dalam keamanan informasi?

KAJIAN PUSTAKA

CIA Triad

Confidentiality, Integrity dan Availability adalah tiga sifat penting dari data dan sering disebut dengan CIA triad. CIA triad dapat berdampak besar dalam sebuah bisnis komputerisasi karena data dapat diartikan sebagai komponen inti untuk berbagai macam bisnis. Data harus dijamin keintegritasannya, dimana pada informasi digital tidak memiliki kerusakan dan hanya dapat diakses oleh yang berwenang atas informasi data tersebut. Jadi Integritas dapat diartikan sebagai keharusan menjaga keakuratan, konsistensi, dan kepercayaan data suatu sistem informasi (Kumar et al., 2018).

CIA triad (Confidentiality, Integrity, Availability) adalah model terkenal untuk pengembangan kebijakan keamanan, digunakan untuk mengidentifikasi masalah dan solusi yang diperlukan untuk keamanan dan sistem informasi (Perrin, 2008).

Kerahasiaan mengacu pada privasi data di mana data milik perusahaan tidak diungkapkan kepada pihak yang tidak berwenang pada setiap kesempatan. Integritas data mengacu pada keyakinan bahwa data yang disimpan di cloud tidak dipermainkan oleh pihak yang tidak berwenang. Itu juga berlaku ketika data dalam perjalanan. Ketersediaan data mengacu pada janji bahwa setiap kali perusahaan membutuhkan data, data tersebut harus tersedia bagi mereka tanpa penundaan atau penolakan. Ketiga sifat keamanan data dasar ini banyak diuji dalam model penyebaran cloud publik.

Otentikasi adalah bukti bagi seseorang untuk mengakses datanya sendiri. Otorisasi adalah tindakan menentukan apakah seseorang memiliki hak untuk melakukan aktivitas pada data seperti membaca atau menulis. Pengguna harus diautentikasi sebelum melakukan aktivitas yang diizinkan untuk mereka lakukan. Non Repudiation adalah jaminan bahwa pengguna yang diautentikasi tidak dapat menyangkal setelah melakukan pekerjaan (Kumar et al., 2018).

Berdasarkan penelitian dari jurnal (Dani, 2008) selama lebih dari 20 tahun, sistem informasi dibangun atas tiga prinsip utama yaitu Confidentiality (kerahasiaan), Integrity (integritas) dan Availability (ketersediaan) atau biasa dikenal dengan CIA triad yaitu :

A. *Confidentiality* (Kerahasiaan)
Confidentiality adalah upaya usaha untuk mencegah terungkapnya informasi yang bersifat rahasia dan sensitif. Beberapa mekanisme yang digunakan guna menjaga konsep *Confidentiality* adalah (Osborne, 2006);
1. Mengklasifikasikan Data
Adalah cara melabelkan informasi guna setiap individu mengetahui siapa yang diizinkan siapa yang berwenang untuk melihat suatu informasi.
2. Enkripsi
Adalah cara yang digunakan untuk menjaga kerahasiaan
3. Pemusnahan Peralatan (Equipment Disposal)
Adalah cara untuk melindungi kerahasiaan suatu informasi saat tidak lagi digunakan dalam media penyimpanan.

B. *Integrity* (Keamanan)
Integrity atau keamanan adalah dimana data tidak bisa diganti, dibuat atau dihapus tanpa adanya proses otorisasi. *Integrity* merupakan prinsip yang ditujukan untuk menjaga keakuratan suatu informasi (Osborne, 2006). Dengan tujuan yaitu (Dani, 2008):
1. Mencegah modifikasi informasi dari user atau pengguna yang tidak memiliki hak.
2. Mencegah akses yang tidak sah atau modifikasi informasi yang tidak disengaja dari pengguna yang tidak memiliki hak.
3. Pemilihan konsistensi Internal dan Eksternal.

Contoh usaha yang dapat dilakukan untuk menjaga integritas suatu dan atau informasi yaitu (Dani, 2008):
1. Checksums
Adalah serangkaian angka yang dihasilkan melalui fungsi matematika untuk memastikan bahwa blok data yang diberikan tidak berubah.
2. Kontrol Akses
Adalah mekanisme untuk memastikan bahwa pihak tertentu hanya dapat melakukan sejumlah aksi tertentu.

C. *Availability* (Ketersediaan)
Menurut (Dani, 2008) *Availability* memastikan agar sistem yang berhak memiliki akses tanpa adanya interupsi sistem dan jaringan dengan memastikan agar informasi atau sumber daya akan selalu tersedia ketika dibutuhkan.

Bentuk-bentuk usaha untuk menjaga ketersediaan antara lain:

1. Redundant *system* atau implementasi berganda pada sistem kedalam suatu infrastruktur
2. Penerapan perangkat IPS guna mencegah ancaman serangan tertentu seperti DDoS yang dapat mengganggu layanan.

Variabel CIA triad sudah pernah diteliti oleh peneliti sebelumnya diantaranya ialah: (Kumar et al., 2018) (Perrin, 2008), (Dani, 2008)

Keamanan Informasi dan Data

Dalam Jurnal (Galih, 2019) mengenai Keamanan informasi menurut Mcleod dan Scheel memiliki tujuan untuk mencapai kerahasiaan, ketersediaan dan integritas (McLeon & Scheel, 2008).

Menurut Sarno dan Iffano Keamanan informasi merupakan upaya untuk melindungi aset informasi dari potensi ancaman. Keamanan informasi secara tidak langsung memastikan kelangsungan bisnis, mengurangi risiko yang muncul, dan memungkinkan untuk mengoptimalkan laba atas investasi. Ada tiga elemen keamanan sistem informasi yaitu kerahasiaan, integritas, dan ketersediaan (Puriwigati, Buana, 2020).

a. Kerahasiaan adalah aspek yang menjamin adanya kerahasiaan data dan sumber informasi. Perlu ada kepastian bahwa suatu informasi hanya dapat di akses oleh orang yang berwenang atau punya hak akses untuk menjamin kerahasiaan informasi yang dikirim.
b. Integritas adalah aspek yang menjamin bahwa informasi tidak dapat diubah tanpa seizin pihak berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integritas.
c. Ketersediaan adalah aspek yang menjamin bahwa informasi akan tersedia saat dibutuhkan oleh pihak berwenang atau yang memiliki hak akses dan memastikan pengguna yang berhak tersebut dapat mengakses informas

Keamanan sistem informasi (Betty Yel & M Nasution, 2022) merupakan aset yang harus dilindungi keamanannya. Keamanan diartikan sebagai “quality or state of being secure to be free from danger”. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya dengan tinjauan sebagai berikut:

Physical Security yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

a. Personal *Security* yang *overlap* dengan “*physical Security*” dalam melindungi orang – orang dalam organisasi.
b. *Operation* untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain.
c. *Identification* Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. *Security* yang Identifikasi umumnya dilakukan dengan penggunaan user name dan user ID.
d. *Authentication*, Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang diklaim.
e. *Accountability* Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu. Keamanan mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan
f. *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.

g. *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi. Perlindungan pada Informasi tersebut dilakukan untuk memenuhi aspek keamanan informasi

Aspek-aspek keamanan informasi (Betty Yel & M Nasution, 2022) seharusnya dikontrol untuk perlindungan informasi yang terkait dengan keamanan informasi yaitu:

a. *Confidentiality* (kerahasiaan) Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
b. *Integrity* (integritas) Aspek yang menjamin bahwa data tidak dirubah tanpa ada izin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *Integrity* ini.
c. *Availability* (ketersediaan) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan,memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait.

Variabel Keamanan dan Informasi data sudah pernah diteliti oleh peneliti sebelumnya diantaranya ialah: (McLeon & Scheel, 2008), (Betty Yel & M Nasution, 2022)

Tabel 1: Penelitian Terdahulu

Penulis (tahun)	Hasil Riset terdahulu	Persamaan dengan artikel ini	Perbedaan dengan artikel ini
(Hermawan[1] et al., 2022)	Konsep CIA Triad dapat menunjukan standar keamanan dan data informasi.	Konsep CIA Triad bisa digunakan untuk dijadikan standar keamanan data informasi.	Tidak ada perbedaan
(Coss & Samonas, 2014)	Konsep CIA Triad berfokus untuk melindungi integritas data yang berada pada suatu *system*.	CIA Triad juga berfokus dengan tujuan untuk melindungi data yang berada pada suatu sistem.	Tidak ada perbedaan
(Arnomo, 2019)	Konsep CIA Triad dapat menjadi kriteria keamanan dan informasi data.	CIA Triad dapat dijadikan kriteria dalam menjaga keamanan dan informasi data.	Tidak ada perbedaan
(Kolkowska et al., 2009)	Konsep CIA Triad bersifat umum dan gagal digunakan dalam standar keamanan informasi.	CIA Triad dijadikan bahan uji coba sebagai standar keamanan informasi.	Cia Triad dinilai berhasil digunakan dalam standar keamanan informasi.

(Qadir & Quadri, 2016)	Yang paling penting dalam konsep CIA Triad adalah *Availability*.	*Availability* adalah salah satu prinsip penting dalam CIA Triad.	*Confidentiality*, *Integrity*, dan *Availability* memiliki peranan yang sama pentingnya dalam konsep CIA Triad.
(Lundgren & Möller, 2019)	Konsep CIA Triad tidak sesuai dengan analisis keamanan karena tidak cukup fleksibel untuk setiap informasi *system* dan organisasi yang berbeda.	CIA Triad dijadikan bahan uji coba sebagai standar keamanan informasi.	Konsep CIA Triad dinilai cukup aman dengan sistem informasi.
(Kaaffah et al., 2022)	Konsep CIA Triad membantu dalam pengamanan dokumen dimana hal tersebut adalah fungsi *Integrity*.	CIA triad dapat membantu dalam pengamanan dokumen (Fungsi *Integrity*)	Tidak ada perbedaan
(Dwinanto & Setiyani, 2021)	Konsep CIA Triad dapat meminimalisir ancaman pada *computer* OS Linux Fedora dengan pembaruan *system*, pengecekan data dan pemisahan user.	Konsep CIA dapat membantu meminimalisir ancaman pada *computer*, pengecekan data dan pemisahan user.	Tidak ada perbedaan
(Agustina et al., 2011)	Kerahasiaan (*Confidentiality*) integritas (*Integrity*), dan ketersediaan (*Availability*) sistem atau informasi adalah tujuan utama dari keamanan	CIA merupakan tujuan utama dari keamanan.	Tidak ada perbedaan
(Sholikhatin et al., n.d.)	Keamanan Informasi menyangkut pada konsep *Confidentiality*, *Integrity* dan *Availability*	Konsep CIA Triad menyangkut pada keamanan Informasi	Tidak ada perbedaan

`

(Salisbury et al., 2015)	Konsep CIA triad dapat menentukan sejauh mana keamanan informasi dalam sistem pembelajaran web kurikulum	CIA Triad dapat menentukan seberapa jauh sistem keamanan informasi.	Jurnal ini tidak menggunakan sampel Web Kurikulum.
(Indrawanti et al., 2018)	Konsep CIA triad dapat dijadikan parameter sebagai bahan pertimbangan untuk membangun suatu keamanan data sistem informasi	Keamanan sistem data informasi dapat menggunakan parameter CIA Triad	Tidak ada perbedaan
(Pu et al., 2023)	Konsep CIA triad menjadi pemandu analisis dalam pembuatan robot industri bagi keamanan data *system* informasi.	CIA Triad dapat menjadi pemandu dalam keamanan data dan informasi.	Jurnal ini tidak menggunakan variabel industri robot.
(Bitzer et al., 2021)	Konsep CIA triad berkaitan dengan ISP, yang mendukung strategi keamanan informasi.	*Confidentiality*, *Integrity*, dan *Availability* dapat mendukung strategi keamanan data dan informasi.	Tidak ada perbedaan.
(Kamal, 2022)	CIA Triad meningkatkan sikap skeptis sehingga auditor lebih sensitif terhadap gejala *fraud*.	Konsep CIA Triad dapat mencegah adanya kecurigaan terhadap kecurangan dalam data dan informasi.	Jurnal ini tidak menggunakan variabel auditor.

METODE PENELITIAN

Dalam proses penulisan artikel ini adapun metode yang digunakan yaitu dengan menggunakan metode kualitatif dan kajian pustaka. Dengan mempelajari serta memahami konsep dan relasi dari setiap variabel yang digunakan berdasarkan artikel-artikel terdahulu yang telah dipublikasikan di Internet melalui Google Cendekia dan media internet lainnya, kemudian diolah menggunakan aplikasi Mendeley.

HASIL DAN PEMBAHASAN

Pentingnya CIA Triad

Berdasarkan hasil penelitian terdahulu,Konsep CIA Triad Confidentiality (Kerahasiaan), Integrity(Integritas), dan Availability (Ketersediaan) diketahui sangat penting dalam keamanan informasi dan data. Dengan kata lain, dengan adanya CIA Triad dapat mencegah terjadinya kejahatan teknologi atau Cyber Crime. CIA Triad dapat menjadi pedoman, landasan, pemandu dan standar keamanan sistem informasi dan data.

Indikator Confidentiality berfokus pada block direct, Integrity berfokus pada aspek filter data dan pengguna, Availability berfokus pada aspek autentikasi. Cia Triad dapat dijadikan indikator keamanan informasi yang digunakan para ahli sebagai alat ukur keamanan sebuah web app (Hermawan1 et al., 2022).

Keamanan sebuah data dapat dapat dipastikan keamanannya karena memenuhi kriteria keamanan informasi yang mengacu pada ‘’CIA Triad’’ yaitu: ‘’Confidentiality’’ (hanya administrator yang mengetahui keberadaan data; ‘’Integrity’’ (terbukti tidak adanya perubahan data), ‘’Availability’’ (data tersedia bagi pengguna dan setelah dilakukannya restore) (Arnomo, 2019).

Penggunaan komputer dalam kegiatan sehari-hari haruslah diimbangi dengan kesadaran pada pengguna akan artinya keamanan komputer. Dengan berpedoman pada pada komponen Confidentiality, Integrity, dan Availability (CIA) sehingga ancaman yang mengancam komputer bisa dikurangi atau diminimalisir (Dwinanto & Setiyani, 2021).

CIA Triad dapat membantu dalam pengaman dokumen, sehingga siapapun yang mencoba meragukan keamanan tersebut dapat terjawab dengan menggunakan sistem ini. Kepercayaan antar pihak yang berbagi informasi meningkat dan jika terdapat masalah konsep ini dapat menjadi bukti kebenaran sistem informasi dan data sesuai salah satu konsep CIA Triad yaitu Integrity (Kaaffah et al., 2022).

Ketika teknologi berkembang dan berbagai jenis teknologi, maka aspek CIA Triad akan lebih dominan daripada yang lainnya. CIA Triad telah mengalami proses rekonfigurasi yang baik, untuk mengakomodasi pertumbuhan eksponensial teknologi informasi dan perubahan signifikan terhadap keamanan dengan fokus data dan informasi dan akhir-akhir ini sebagai perlindungan keamanan dari cyber. (Coss & Samonas, 2014).

Dalam penerapan keamanan informasi, pemangku kepentingan keamanan harus memperlakukan tiga atribut yaitu keamanan, kerahasiaan, integritas dan ketersediaan. Ketersediaan merupakan yang terpenting dari ketiga aspek di atas, fakta dimana dunia bergantung pada ketersediaan, tanpa adanya ketersediaan seseorang tidak dapat menjalankan dan menerapkan konsep kerahasiaan dan integritas tanpa informasi yang tersedia (Qadir & Quadri, 2016).

CIA Triad berperan penting dalam menjaga sistem informasi dan data, hasil ini sesuai dengan riset yang sudah dilakukan terdahulu oleh : (Hermawan1 et al., 2022), (Arnomo, 2019), (Dwinanto & Setiyani, 2021), (Kaaffah et al., 2022), (Coss & Samonas, 2014), (Qadir & Quadri, 2016).

Pentingnya Keamanan Sistem Informasi dan Data

Informasi dan data adalah aset yang paling penting dalam suatu organisasi maupun perusahaan. Aset-aset yang penting tentunya harus dijamin keamanannya dan harus memiliki sistem yang selalu melindungi aset aset tersebut. Maka harus dibentuk suatu sistem yang dapat menjamin keamanan informasi dan data dengan sistem yang dibentuk. Keamanan informasi dan data dapat menjamin kesuksesan organisasi maupun perusahaan yang diolah sedemikian rupa guna mengantisipasi serta melindungi data dan informasi dari pihak pihak yang bertanggung jawab.

Keamanan data dan informasi sering menjadi masalah yang sering ditemukan dalam perusahaan maupun organisasi yang sedang berkembang. Tidak sedikit kejahatan dalam sistem informasi dan data menjadi suatu hal yang dapat menjatuhkan perusahaan maupun organisasi yang sengaja dilakukan oleh pihak atau individu yang ingin membuat suatu

organisasi atau perusahaan mengalami suatu masalah dan menciptakan masalah di dalam nya. Oleh karena itu keamanan sistem informasi dan data harus diprioritaskan.

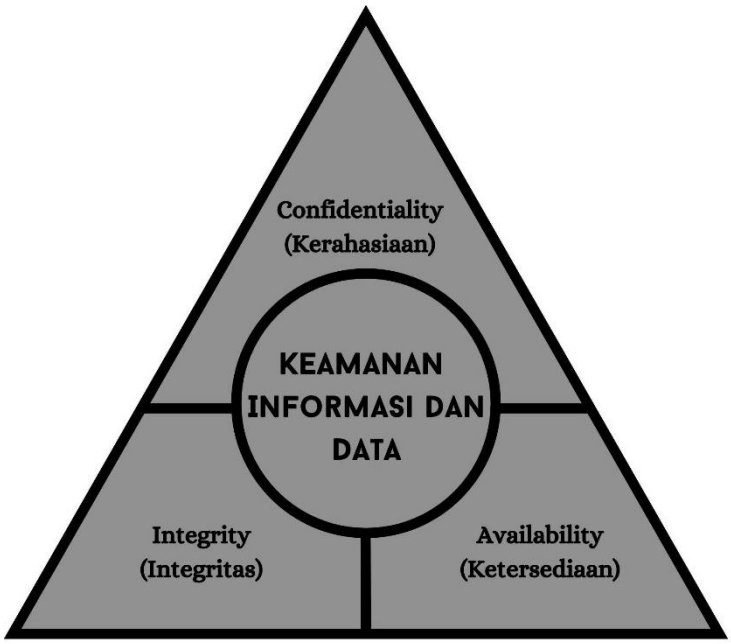
Dalam penelitian ini kita dapat melihat bahwa indikator-indikator yang ada dalam pembentukan keamanan sistem informasi dan data sangatlah penting dan sangat erat kaitan nya antara satu sama lain.

Keamanan yang dibentuk tentunya tidak hanya dapat melindungi aset informasi dan data saja, tetapi juga menjaga fungsi kegiatan atau bisnis dalam suatu perusahaan maupun organisasi tersebut (Agustina et al., 2011).

Keamanan informasi menekankan pentingnya tiga persyaratan dasar: kerahasiaan (yaitu, hanya tim yang memiliki privilege yang dapat melihat informasi yang dibatasi), integritas (hanya tim yang memiliki privilege yang dapat mengubah informasi yang dibatasi) dan ketersediaan (semua individu dengan privilege yang sesuai harus memiliki akses langsung ke informasi terbatas) (Salisbury et al., 2015).

Keamanan Sistem Informasi dan Data merupakan tujuan utama diterapkannya konsep CIA Triad, hasil ini sesuai dengan riset yang sudah dilakukan oleh : (Qadir & Quadri, 2016), (Qadir & Quadri, 2016).

CONCEPTUAL HOMEWORK



Gambar 1.1 CIA Triad Keamanan Informasi dan Data

Berdasarkan gambar 1.1 adalah konsep perumpamaan hubungan dan kaitan CIA TRIAD dalam melindungi keamanan informasi dan data dalam suatu sistem yang diterapkan. Ketiga faktor ini saling berkaitan dan saling menjaga ikatan satu sama lain, dengan kata lain jika salah satu faktor tersebut dihilangkan Keamanan informasi dan data akan sangat beresiko. Maka dari itu keterkaitan CIA Triad memiliki peran yang sangat penting dalam menjaga keamanan sistem informasi dan data.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil pembahasan dan analisis pada jurnal yang telah terdahulu, dapat diambil beberapa kesimpulan, sebagai berikut:

1. CIA Triad dalam sistem informasi dan data sangat penting dijadikan pedoman atau dasar kerangka kerja, karena didalamnya terdapat indikator dalam pencegahan terjadinya Cyber Crime yang dapat merugikan organisasi atau perusahaan.
2. CIA Triad mencakup tiga aspek penting keamanan informasi. Dengan mempertimbangkan semua aspek ini, organisasi dapat mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan secara holistik.
3. Dengan menerapkan dan menjadikan CIA Triad sebagai pedoman, organisasi dapat menciptakan lingkungan yang aman bagi informasi dan data mereka. Ini membantu meningkatkan kepercayaan dan keandalan bagi pengguna, klein, dan mitra bisnis.

Saran

Berdasarkan hasil jurnal diatas, dapat diberikan beberapa saran, sebagai berikut:

1. Manfaatkan teknologi keamanan seperti enkripsi data, firewall, dan sistem deteksi intrusi untuk melindungi informasi dan data dari ancaman yang mungkin timbul.
2. Lakukan evaluasi keamanan informasi secara rutin untuk mengidentifikasi kerentanan dan memastikan kepatuhan terhadap kebijakan keamanan. Tindakan perbaikan yang tepat harus diambil untuk mengatasi temuan dan meningkatkan keamanan.

BIBLIOGRAPHY

Agustina, D., Pramadista, F., & Regyna, T. (2011). Manajemen keamanan informasi. 1, 1–19. https://doi.org/12.01.123

Arnomo, I. (2019). Simulasi Backup Dan Restore Database Repository. Jurnal Sistem Informasi, Teknologi Informasi Dan Komputer, 9(2), 92–99.

Betty Yel, M., & M Nasution, M. K. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. Jurnal Informatika Kaputama (JIK), 6(1), 92–101.

Bitzer, M., Brinz, N., & Ollig, P. (2021). Disentangling the Concept of Information Security Properties: Enabling Effective Information Security Governance. ECIS 2021 Research Papers, 134(May), 1–18. https://aisel.aisnet.org/ecis2021_rp/134

Coss, D., & Samonas, S. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. Journal of Information System Security, 10(3), 21–45. www.jissec.org

Dani, J. (2008). Pengembangan Kebijakan Keamanan Informasi Pada Perusahaan Jasa Layanan Kurir : Studi Kasus Pt. Ncs. 6–26.

Dwinanto, I., & Setiyani, H. (2021). Implementasi Keamanan Komputer pada Aspek Confidentiality, Integrity, Availibility (CIA) Menggunakan Tools Lynis Audit System. Jurnal Maklumatika, 8(1), 35–46.

Galih, A. (2019). Experience: Data and information quality challenges in governance, risk, and compliance management. Journal of Data and Information Quality, 11(2). https://doi.org/10.1145/3297721

Hermawan1, A., Hartati2, T., & Wijaya3, Y. A. (2022). Analisa Keamanan Data melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad. 7(3), 125–130.

Indrawanti, A. S., Azinar, A. W., & Firdiansyah, M. A. (2018). SECURE E-VOTING MENGGUNAKAN METODE RSA DAN. 4(1), 67–75.

Kaaffah, F. M., Maulana, R., Zulfikar, W. B., Slamet, C., Lukman, N., & Rahman, A. (2022). Integrity Assurance System for Document Security Using Keccak and Quick Algorithm Response Code. Proceeding of 2022 8th International Conference on Wireless and Telematics, ICWT 2022. https://doi.org/10.1109/ICWT55831.2022.9935362

Kamal, A. (2022). Teknologi Informasi dan Skeptisisme Profesional terhadap Fraud Detection Skills Auditor Internal Pemerintah. YUME : Journal of Management, 5(2), 295–313. https://doi.org/10.2568/yum.v5i2.1639

Kolkowska, E., Hedström, K., & Karlsson, F. (2009). Information Security Goals in a Swedish Hospital Ella Kolkowska, Karin Hedström, Fredrik Karlsson Örebro University, Sweden. Security, Assurance and Privacy: Organisational Challenges. Proceedings of the 8th Annual Security Conference, 1–11.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science, 125(January), 691–697. https://doi.org/10.1016/j.procs.2017.12.089

Lundgren, B., & Möller, N. (2019). Defining Information Security. Science and Engineering Ethics, 25(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Pu, H., He, L., Cheng, P., Chen, J., & Sun, Y. (2023). Reference : To appear in : Received Date : Revised Date : Accepted Date : Systems Science — Article CORMAND2 : A Deception Attack Against Industrial Robots. Engineering. https://doi.org/10.1016/j.eng.2023.01.013

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security, 07(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Salisbury, W. D., Ferratt, T. W., & Wynn, D. E. (2015). Assessing the Emphasis on Information Security in the Systems Analysis and Design Course.

Sholikhatin, S. A., Setyanto, A., Si, S., Luthfi, E. T., & Kom, M. (n.d.). Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus : Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto). 4(1), 1–9.