e-ISSN 2962-1968

Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp

Reni Kuswulandari[1*], Axzara Wirid Isra Jowanka [2], Telaga Nabila Putri Riyanto[3], Titin Listiani[4]

[1,2,3,4] *Sistem Informasi*
Universitas Duta Bangsa Surakarta
[1]202020271@mhs.udb.ac.id, [2]202020889@mhs.udb.ac.id,
[3]202030234@mhs.udb.ac.id, [4]202021221@mhs.udb.ac.id

Abstrak— **Kejahatan siber telah menjadi ancaman yang signifikan dalam era digital saat ini. Keberadaan WhatsApp juga rentan terhadap berbagai risiko keamanan dan ancaman kejahatan siber. Tidak adanya pengetahuan tentang kesadaran bermain media social membuat tidak sedikit para pengguna menjadi korban kejahatan siber (cybercrime). Penelitian ini bertujuan untuk melakukan analisis mendalam terhadap risiko-risiko kejahatan siber yang dapat mempengaruhi pengguna WhatsApp dan memberikan langkah-langkah pencegahan yang tepat untuk mengurangi dampak negatif dari ancaman tersebut. Metode yang digunakan dalam penelitian ini adalah kualitatif dengan penelitan mendalam menggunakan observasi untuk mengamati dan mempelajari perilaku pengguna. Berdasarkan analisis data pada penelitian ini data yang dicuri berkisar dari informasi pribadi dan SMS hingga informasi perbankan rahasia seperti one-time password (OTP).**
Kata kunci— Kejahatan siber, manajemen risiko, Whatsapps, analisis risiko

Abstract— **Cybercrime has become a significant threat in today's digital age. The existence of WhatsApp is also vulnerable to various security risks and cybercrime threats. Lack of knowledge about awareness to be careful playing social media makes not a few users become victims of cybercrime. This research aims to conduct an in-depth analysis of the cybercrime risks that can affect WhatsApp users and provide appropriate preventive measures to reduce the negative impact of these threats. The method used in this research is qualitative with in-depth research using observation to observe and study user behavior. Based on the data analysis in this study, the stolen data ranges from personal information and SMS to confidential banking information such as one-time passwords (OTP).**
Keywords— Cybercrime, risk management, Whatsapps, risk analysis

I. PENDAHULUAN

Saat ini, perkembangan teknologi sudah berkembang. Disaat ada perkembangan baru akan ada sisi buruk saat menggunakan teknologi, yang mengakibatkan akan kejahatan dengan media komputer. Kejahatan tersebut merupakan cybercrime. Beberapa lembaga keamanan siber di Indonesia. Di Indonesia salah satunya adalah Badan Siber dan Sandi Negara (BSSN). (BSSN, 2019a) [1]

Cybercrime merupakan kejahatan dilakukan dengan menggunakan komputer atau jaringan komputer sebagai alatnya, sasaran dan TKP, juga penipuan online, pelecehan, penipuan identitas dan lain-lain [4]. Cybercrime ada dampak negatif yang mempengaruhi perkembangan Internet of Things, dimana Internet of Things merupakan konsep penggunaan Internet untuk banyak hal tanpa harus bertemu [2].

Saat ini, ancaman kejahatan dunia maya terjadi, salah satu perhatian utama saat menggunakan perangkat lunak dan platform komunikasi online, kejahatan dunia maya yang terjadi berupa pencurian identitas, intimidasi, penipuan dan pencurian online. Cybercrime sering terjadi dikarenakan banyak pengguna yang tidak sadar menggunakan media sosial [3].

Aplikasi paling populer di dunia adalah WhatsApp, dengan sejukah fitur komunikasi seperti pesan teks, panggilan suara, panggilan video, dan berbagi media. Dengan seiring dengan pertumbuhan penggunaan WhatsApp, ancaman kejahatan dunia maya ikut meningkat. Manajemen risiko merupakan cara sistematis untuk mengidentifikasi, menganalisis, dan mengurangi risiko yang dapat memengaruhi organisasi atau individu. Di aplikasi WhatsApp, manajemen risiko penting agar dapat melindungi pengguna dari berbagai ancaman kejahatan dunia maya.

Oleh karena itu, analisis manajemen risiko terhadap ancaman kejahatan siber dalam aplikasi WhatsApp menjadi suatu kebutuhan yang mendesak. Risiko yang mungkin terjadi mencakup serangan malware, phishing, peretasan akun, pencurian data pribadi, dan penyebaran informasi palsu. Dalam rangka mengurangi risiko ini, praktik manajemen risiko yang efektif perlu diimplementasikan.

e-ISSN 2962-1968

Risiko yang dihadapi dalam menghadapi ancaman cybercrime berasal dari dalam negeri dan dari luar dengan menggunakan perkembangan sosial, politik, budaya, ideologi dan teknologi [4]. Ketika kejahatan komputer terjadi, polisi menyita dua barang bukti, yaitu barang bukti digital dan artefak [5].

Tujuan penelitian ini merupakan untuk melihat dan menganalisis praktik manajemen risiko berupa ancaman kejahatan dunia maya pada penggunakan WhatsApp. Faktor-Faktor yang Mempengaruhi Pengguna WhatsApp Sebagai Subyek Penelitian Metode penelitian observasi yang sebagai bahan untuk mengumpulkan informasi dengan cara melihat perilaku pengguna selama menggunakan aplikasi WhatsApp, memberitau ancaman cybercrime dan berinteraksi dengan konten yang mereka terima. Hasil penelitian ini semoga dapat memberikan pemahaman yang lebih mendalam mengenai risiko kejahatan dunia maya saat menggunakan WhatsApp dan memberikan kontribusi yang berharga bagi pengembangan praktik manajemen risiko yang lebih efektif.

II. METODOLOGI PENELITIAN

Metodologi riset ini ialah suatu ilmu yang menekuni cara-cara melaksanakan pengamatan yang bermakna dalam langkah-langkah terpadu yang tersusun secara ilmiah buat mencari, mengumpulkan, menganalisis, serta mendapatkan data sehingga bisa digunakan buat menciptakan meningkatkan serta menguji kebenaran informasi. 6].

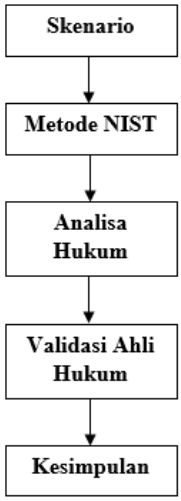
Riset ini memakai riset kualitatif, yang mana riset kualitatif ialah tata cara ilmiah yang kerap digunakan oleh sekelompok periset di bidang ilmu sosial. Riset kualitatif buat mengumpulkan pengetahuan lewat uraian serta temuan Tata cara riset kualitatif merupakan proses penyelidikan serta uraian yang bersumber pada tata cara menekuni fenomena sosial serta permasalahan manusia. Riset melalui manajemen risiko Analisis kejahatan dunia maya pada aplikasi WhatsApp penuhi ciri riset kualitatif, pada spesialnya pengungkapan data secara mendalam dengan mengamati aktivitas informan.

1. Observasi / Pengamatan

Dalam perihal ini periset melaksanakan observasi langsung, atau observasi terhadap korban penipuan melalui PDF yang diunduh di aplikasi WhatsApp. Dengan mengamati secara nonpartisipatif, yang artinya peneliti hanya bertindak selaku pengamat fenomena yang sudah diteliti. Pengamatan yanh dicoba secara langsung supaya memperoleh cerminan universal tentang tujuan riset.

Tata cara pengujian yang digunakan di riset ini merupakan National Institute of Standards and Technology (NIST). NIST memiliki metodologi empat langkah untuk menyelesaikan dan menyelidiki kasus kejahatan dunia maya. Langkah pertama terdiri dari pengumpulan (pengumpulan informasi), investigasi (pemeriksaan bukti), analisis, dan terakhir pelaporan (analisis hubungan).[7]

Terdapat sebagian tahapan ataupun prosedur riset ini ialah yaitu:



Gambar 1. Diagram Alur Prosedur Penelitian

III. HASIL DAN PEMBAHASAN

Dari sekian banyak orang yang memakai internet di dunia, spesialnya di Indonesia, tidak dapat dipungkiri kalau orang yang sangat banyak memakai serta sangat memerlukan Internet dikala ini merupakan dari golongan mahasiswa. Dari banyak nya jumlah pengguna Internet di golongan mahasiswa tersebut, jumlah kejahatan terjalin di dunia internet, pula diketahui selaku cyber crime pula terus menjadi banyak terjalin Perihal ini bisa jadi saja terjalin sebab minimnya pengetahuan tentang bahaya yang hendak terjalin di Internet

e-ISSN 2962-1968

ataupun metode buat mengamankan diri mereka dari bahaya yang terletak di dunia Internet[8].

Oleh sebab itu, penelitian yang dilakukan menggunakan studi kasus mahasiswa "S" telah mengalami kejahatan online melalui WhatsApp.

Kemudian terdapat beberapa langkah atau metode penelitian dalam penelitian ini yaitu sebagai berikut :

1. Skenario

Awalnya berawal dari akun WhatsApp di ponsel Android, setelah itu Akun A (pelaku) dan Akun B (korban) berbicara kepada pelaku sebagai call center bank ternama dan menggunakan akunnya. Informasi tentang korban penipuan di WhatsApp.

Alur atau tahapan si penipu yaitu telfon menggunakan WhatsApp, konfirmasi data, download file yang berbentuk APK, transfer sejumlah uang ke dana dan peretasan akun dana sehingga pelaku dapat mentransfer sendiri uang ke rekening pribadi.

2. Metode NIST

Kemudian karena pada penelitian ini menggunakan metode penelitian NIST, yaitu sebuah metode yang memiliki empat tahapan dalam menyelesaikan dan menyelidikan kasus Cyber Crime, tahap pertama yaitu:

a) Collection (Pengumpulan Data)
b) Pengumpulan data yang akan kita kumpulkan adalah mengumpulkan barang bukti pada korban.
c) Examination (Pemeriksaan barang bukti)
d) Pemeriksaan barang bukti ini adalah sebagai bentuk untuk membuktikan apakah barang bukti yang ada valid atau tidak dengan alur skenarionya.
e) Analysis
f) Setelah data sudah valid, kemudian kita melakukan analisis tentang bagaimana cara si pelaku menipu korban, atau menggunakan system atau alat seperti apa untuk menipu korban dan bagaimana pengamanannya terhadap penggunaan social media seperti penggunaan WhatsApp serta menganalisis data yang lain.
g) Reporting (Membuat laporan berdasarkan hasil analisis)

3. Analisa Hukum

Sumber bahan hukum yang digunakan berasal dari penelitian kepustakaan berupa sumber hukum primer berdasarkan peraturan perundang-undangan di bidang informasi dan transaksi elektronik yaitu UU No. 19/2016 mengubah UU Informasi dan Transaksi Elektronik No. 11, 2008. [9].

Serta ada pasal 378 KUHP menerangkan bahwa Penipuan mengacu pada suatu keadaan yang dilakukan oleh seseorang dengan maksud buat menguntungkan diri sendiri ataupun orang lain secara melawan hukum dengan memakai nama ataupun martabat palsu, penipuan ataupun apalagi kebohongan buat menarik orang lain ke dalam tangannya. memberinya sesuatu atau utang, atau membatalkan klaim, diancam dengan hukuman penjara hingga empat tahun karena penipuan**.**

4. Validasi Ahli Hukum

Ruang lingkup kejahatan ini tidak tetap dan dapat berubah-ubah tergantung ada tidaknya penyimpangan atau hukum pidana membuat ketentuan khusus tentang zat tertentu. Unsur-unsur kejahatan dapat dibedakan sekurang-kurangnya dari dua segi, yaitu: (1) dari segi teoretis; (2) dari segi hukum. Sarana teoretis berdasarkan pendapat para ahli hukum tercermin dalam rasionalitas ungkapan. Oleh sebab itu, fokus hukum adalah bagaimana untuk merumuskan realitas kejahatan sebagai kejahatan khusus dalam ketentuan peraturan perundang-undangan yang sudah berlaku.

5. Kesimpulan

Modus dari pelaku yaitu pelaku mengirimkan file. Aplikasi dan meminta calon korban untuk masuk dengan cara klik link untuk menginstal. Setelah apliaksi terinstall korban harus mengizinkan akses ke sejumlah aplikasi yang menguntungkan pelaku untuk mencuri informasi rahasia dari perangkat calon korban.

Informasi yang dicuri berkisar dari informasi pribadi dan pesan teks hingga informasi rahasia perbankan seperti one-time password (OTP).

Agar tidak tertipu penipuan ini, ada tiga hal penting yang harus diperhatikan, yaitu:

e-ISSN 2962-1968

a. Jangan mengklik file .APK yang Anda terima sebagia pesan instan dari orang asing
b. Selalu pastikan bahwa sumber aplikasi yang anda pasang adalah dari Google Play Store atau sumber yang terpercaya.
c. Jika aplikasi yang akan diinstal bukan dari sumber tepercaya, jangan berikan akses apa pun.

Ada Beberapa langkah yang dapat Anda lakukan untuk menghindari serangan phishing online antara lain:

a. Meningkatkan kewaspadaan organisasi terhadap ancaman dunia maya
b. Mengimplementasikan standar keamanan jaringan informasi di seluruh organisasi
c. Melatih SDM untuk mempertahankan keterampilan keamanan siber
d. Terapkan arsitektur sistem dan layanan yang aman dan perbarui secara teratur.
e. kemungkinan pencegahan, mitigasi dan koreksi dan revisi.

Keamanan dunia maya menjadi prioritas utama bagi negara-negara di seluruh dunia karena teknologi informasi dan komunikasi diterapkan di berbagai bidang antara lain masyarakat, ekonomi, hukum, kesehatan, pendidikan, budaya, pemerintahan, keamanan, pertahanan. DLL. ada. Berbanding lurus dengan pentingnya penggunaan TIK, risiko dan bahaya penyalahgunaannya telah tumbuh dan menjadi semakin kompleks. [10].

Ada cara umum di web saat ini untuk menghindari penipuan pesan WhatsApp. Disini OJK menawarkan beberapa tips menghindari penipuan hal tersebut:

a) Hati-hati saat mengunduh aplikasi baca yang detail tentang aplikasi, Jangan langsung klik link yang berupa file apk
b) Mengunduh aplikasi resmi di Play Store
c) Jangan lupa untuk mengecek keaslian nomor telepon pengirim. Jika ada yang mengaku sebagai pejabat PLN/BPJS/lembaga/perusahaan, Anda dapat mengajukan pertanyaan dengan menghubungi call center resmi perusahaan.
d) Jangan pernah mengungkapkan username, password, OTP, PIN akun atau nama ibu kandung Anda kepada siapapun.
e) Jangan tanggapi nomor yang tidak dikenal, terutama yang mengirim file mencurigakan (seperti file APK)
f) Selalu periksa riwayat akun anda secara teratur.
g) Ingat untuk mengubah kata sandi Anda secara teratur. Jangan gunakan jaringan Wi-Fi publik untuk transaksi keuangan.

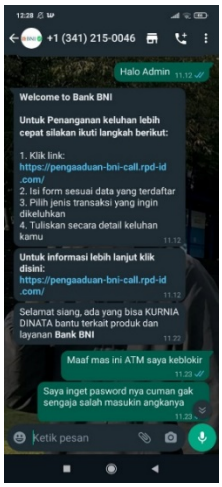
Gambar berikut adalah bukti komunikasi antara korban dan pelaku. Awalnya pada tanggal 01 April 2023 sekitar 20.00 WIB korban melakukan penarikan tunai tetapi karena korban salah memasukkan PIN ATM KIP selama 3 kali dan berakibat ATM korban terblokir. Pada Tanggal 02 2023 korban menghubungi call center yang didapatkan dari internet (google), Kemudian korban mencoba menghubungi nomor tersebut pada jam 11.12 WIB. Seperti bukti pada gambar 2 dibawah ini:

Gambar 2. Bukti Nomor Pelaku Penipuan.

Gambar 3 merupakan percakapan via whastapp dan via telepon, korban disuruh untuk mengirimkan nomor rekening dan nomor ATM KIP dalam bentuk foto. Setelah itu korban disuruh untuk mendownload file dalam bentuk aplikasi (APK) yang berjudul Form Pengaduan.APK.

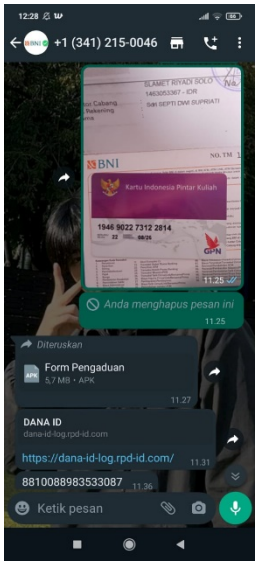
e-ISSN 2962-1968

.



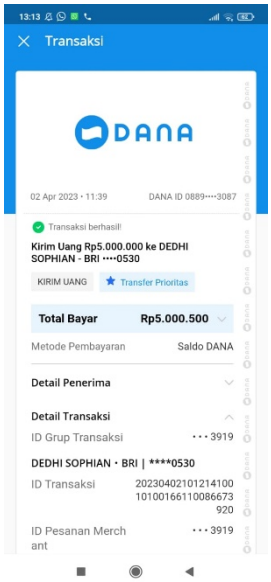
Gambar 3. Bukti komunikasi anatara korban dan pelaku

Selanjutnya korban di minta untuk mentransfer uang sebesar Rp. 5.050.505 dari rekening BNI korban ke akun dana korban. Setelah korban menunggu lama, tanpa disadari akun dana korban tidak bisa di akses. Beberapa menit kemudian korban kembali mengakses akun dananya namun tidak ada saldo masuk, padahal di rekening BNI sudah terdapat status transfer berhasil. Seperti bukti pada gambar 4 dibawah ini:



Gambar 4. Bukti Pelaku Mengirimkan Nomer Rekening.

Pada Gambar 5 korban kembali mengakses akun dana dan berhasil masuk, kemudian korban mencoba membuka bagian bukti transaksi di akun dana yang ternyata disitu terdapat bukti transaksi pengiriman uang dari akun dana korban ke akun BRI atas nama yang berinisial DS.



Gambar 5. Bukti Transaksi Dana ke Rekening Pelaku

Berikut ini adalah alat dan bahan yng digunakan dalam penyidikan forensik ini, ditujukan pada tabel 1.

Tabel 1. Alat dan Peneltian

Alat dan Bahan	Deskripsi/Spesifikasi	Keterangan
laptop	Merk Asus Vivobook A416JA0-FHD311 Intel Core i3	Ada
handphone	Samsung Galaxy A13	Ada
KingRoot	Aplikasi yang digubakan untuk root pada smartpgone android	Ada
WhatsApp Versi 2.23.11.80	Aplikasi instan messenger yang menjadi obyek dari penelitian	Ada
AccessData FTK Imager	Aplikasi yang digunakan untuk melukukan imaging data	Ada

Setelah berhasil menyelesaikan tahap pengumpulan, bukti terkait aplikasi WhatsApp diperoleh. Disini kami akan membahas dan memaparkan bukti-bukti terkait aplikasi WhatsApp untuk mengungkap kasus kejahatan.

e-ISSN 2962-1968

Tabel 2. Bukti berhasil dikumpulkan

Bukti		Penjelasan
Handphone	Samsung Galaxy A13	Terasedia
Nomer Telephon Korban	089342514306	Tersedia
Nomer Handphone Pelaku	+1(341)215-0046	Tersedia
Nama dan Foto Profil WhatsApp	Bank BNI	Tersedia
Percakapan	4	Tersedia
Tahun komunikasi	2023	Tersedia
Bulan komunikasi	April	Tersedia
Tanggal komunikasi	02	Tersedia
Jam Komunikasi	Pukul :11.12 WIB	Tersedia

IV. KESIMPULAN

Manajemen risiko yang di bidang informasi serta komunikasi yang berkaitan dengan hidup orang banyak atau bersifat sangat rahasia merupakan berbagai hal yang dilakukan untuk mengurangi kerawanan salahguna informasi dan data di dunia maya. Bahan hukum yang digunakan berasal dari studi kepustakaan berdasarkan peraturan perundang-undangan di bidang informasi dan transaksi elektronik, UU No.1. Pasal 11 Tahun 2016, Pasal 19 Tahun 2016 dan Pasal 378 KUHP, perubahan UU Informasi dan E-Commerce, menjelaskan bahwa penipuan adalah perbuatan untuk tujuan mencari keuntungan, yang diancam dengan pidana penjara paling lama empat tahun. . Cara kerja pelaku dalam hal ini adalah pelaku mengirimkan file .APK dan meminta calon korban untuk mengklik kemudian menginstal .APK tertentu. Setelah diinstal, calon korban harus mengizinkan akses ke berbagai aplikasi yang dapat digunakan penjahat untuk mencuri data rahasia dari perangkat calon korban. Informasi yang dicuri berkisar dari informasi pribadi dan pesan teks hingga informasi rahasia perbankan seperti one-time password (OTP).

Agar tidak tertipu penipuan ini, ada 3 hal penting yang harus anda diperhatikan, yaitu:

a. Jangan mengklik file .APK yang Anda terima sebagai pesan instan dari orang asing.
b. Selalu pastikan bahwa sumber aplikasi yang Anda pasang adalah dari Google Play Store atau sumber terpercaya.
c. Jika aplikasi yang akan diinstal bukan dari sumber tepercaya, jangan berikan akses apa pun.
d. Untuk itu pada kasus seperti ini, kita atau pelaku yang lain harus meningkatkan kesadaran organisasi terhadap ancaman dunia maya, mengimplementasikan standar keamanan jaringan di seluruh organisasi, melatih sumber daya manusia untuk mempertahankan keterampilan keamanan siber, menerapkan dan memperbarui sistem dan arsitektur layanan yang aman secara teratur, serta memiliki kemampuan pencegahan, mitigasi dan perbaikan, serta audit.

UCAPAN TERIMA KASIH

Puji dan syukur peneliti panjatkan kehadirat Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya yang telah memberikan kesehatan dan kesempatan kepada peneliti sehingga skripsi ini dapat terselesaikan dengan baik. Sebuah majalah dengan judul "ANALISIS MANAJEMEN RISIKO ANCAMAN KEJAHATAN SIBER (CYBER CRIME) DALAM APLIKASI WHATSAPP" disusun untuk memenuhi persyarat Ulangan Akhir Semester mata kuliah Manajemen Resiko pada program studi system informasi. Dalam penyusuna artikel ini, peneliti menemui banyak kendala yang dapat diatasi dengan saran dan dorongan dari berbagai pihak, pada akhirnya dapat menyelesaikan artikel ini, Akhir kata, peneliti berharap semiga bermanfaat dan jadi pembelajaran kita semua.

REFERENSI

[1] Putra, M. A. D. (2020). *Pelacakan Pelaku Kejahatan Siber Pengguna Virtual Private Network (Vpn) Pada Jaringan The Onion Router (Tor)(Studi Kasus Di Badan Siber Dan Sandi Negara)* (Doctoral dissertation, UNIVERSITAS AIRLANGGA).

[2] Dasmen, R. N., & Kurniawan, F. (2021). Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial. *Techno. Com*, *20*(4), 527-539.

[3] Soni, S., Hafid, A., & Sudyana, D. (2019). Analisis Kesadaran Mahasiswa Umri Terkait Penggunaan Teknologi & Media Sosial Terhadap Bahaya Cybercrime. *Jurnal Fasilkom*, *9*(3), 28-34.

[4] Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 35-50.

[5] Widatama, K. (2019). Sistem Monitoring Bukti Digital Untuk Meningkatkan Kontrol Terhadap Kasus Cybercrime Di Indonesia. *INTEK: Jurnal Informatika dan Teknologi Informasi*, *2*(1), 39-46.

[6] Rafie, A. M. (2020). Analisis kesadaran cybersecurity pada pengguna media sosial di Indonesia.

[7] Fitriana, M., Khairan, A. R., & Marsya, J. M. (2020). Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *4*(1), 29-39.

[8] Riyandhika, R. R. (2020). Analisis Kesadaran Cybersecurity pada Kalangan Mahasiswa di Indonesia. *AUTOMATA*, *1*(2).

[9] Singgi, I. G. A. S. K., Suryawan, I. G. B., & Sugiartha, I. N. G. (2020). Penegakan Hukum terhadap Tindak Pidana Peretasan sebagai Bentuk Kejahatan Mayantara (Cyber Crime). *Jurnal Konstruksi Hukum*, *1*(2), 334-339.

[10] Ginanjar, Y. (2022). Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan

Sandi Negara. *Dinamika Global: Jurnal Ilmu Hubungan Internasional*, *7*(02), 295-316