Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume 14 Nomor 2 Edisi Oktober 2024
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek: Identifikasi, Evaluasi, dan Mitigasi Ancaman

Literature Review Cyber Risk Management in Projects: Threat Identification, Evaluation and Mitigation

Milky Gratia Br Sitorus[1], **Novita Maria**[2], **Yunisa Nur Safa**[3*]
Program Studi Teknik Informatika, Universitas Palangka Raya, Kalimantan Tengah, Indonesia
*E-mail: yunisanursafa4s4@gmail.com

Abstrak

Dalam era digital saat ini, proyek-proyek bisnis semakin rentan terhadap ancaman siber yang dapat mengakibatkan kerugian yang cukupbesar, baik itu dari segi finansial maupun reputasi. Jurnal ini membahas pendekatan manajemen risiko siber yang efektif dalam proyek, yang meliputi identifikasi, evaluasi, dan mitigasi ancaman digital. Dengan tujuan, untuk memberikan tinjauan tentang manajemen resiko pada proyek. Pada jurnal ini membahasa tentang bagaimana mengidentifikasi risiko yang dilakukan dengan menganalisis secara menyeluruh berbagai potensi ancaman siber, seperti malware, phishing, dan serangan DDoS yang dapat mempengaruhi proyek. Selanjutnya, ada evaluasi risiko dilakukan dengan menilai tingkat kerentanan dan dampak potensial dari setiap ancaman yang teridentifikasi, menggunakan metode studi literatur. Studi literatur yang digunakan adalah tinjuan literatur yang mecakup analis data-data yang telah didapat yang berupa artikel serta buku yang relavan dengan topik. Tahap terakhir ada mitigasi risiko, yang melibatkan pengembangan strategi untuk mengurangi atau menghilangkan dampak ancaman, seperti penerapan kontrol keamanan, pendidikan dan pelatihan bagi karyawan, serta rencana respons insiden. Studi ini menekankan pentingnya pendekatan proaktif dan holistik dalam manajemen risiko siber untuk memastikan keberhasilan dan keberlanjutan proyek. Jurnal ini bertujuan untuk memberikan tinjauan tentang manajemen resiko pada proyek. Dengan hasil menunjukkan bahwa integrasi praktik manajemen risiko siber yang komprehensif dapat secara signifikan meningkatkan ketahanan proyek terhadap ancaman digital.

Kata kunci*: Keamanan Siber, Manajemen Proyek, Manajemen Risiko Proyek*

Abstract

In today's digital era, business projects are increasingly vulnerable to cyber threats, which can result in significant financial and reputational losses. This journal discusses an effective cyber risk management approach for projects, encompassing the identification, evaluation, and mitigation of digital threats. The objective is to provide an overview of risk management in projects. This journal explains how to identify risks by thoroughly analyzing various potential cyber threats, such as malware, phishing, and DDoS attacks that could impact the project. Subsequently, risk evaluation is conducted by assessing the vulnerability and potential impact of each identified threat, using a literature review method. The literature review includes the analysis of data obtained from relevant articles and books on the topic. The final stage involves risk mitigation, which includes developing strategies to reduce or eliminate the impact of threats, such as implementing security controls, providing employee education and training, and developing incident response plans. This study emphasizes the importance of a proactive and holistic approach to cyber risk management to ensure the success and sustainability of projects. The journal aims to provide an overview of risk management in projects, demonstrating that the integration of comprehensive cyber risk management practices can significantly enhance the resilience of projects against digital threats.

Keywords: *Cyber Security, Management Project, Project Risk Management.*

Naskah diterima 28 Mei 2024; direvisi 22 Jul. 2024; dipublikasikan 01 Okt. 2024.

I. PENDAHULUAN

Pada saat era digital sekarang, organisasi semakin bergantung pada teknologi informasi untuk mendukung operasi dan mencapai tujuan bisnis mereka[1]. Namun, ketergantungan ini juga membawa risiko signifikan terkait dengan keamanan siber. Ancaman digital terus berkembang baik dalam kompleksitas maupun frekuensi, menciptakan tantangan besar bagi manajer proyek dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi dalam proyeknya. Jika tidak ada keamanan jaringan atau sistem informasi, kemungkinan besar terdapat kejadian kehilangan informasi pada organisasi tersebut[2]. Pada konversi yang

diadakan pada 23 mei 2023, Deputi III BSSN Dwi Kardono mengatakan bahwa, semakin tinggi teknologi, semakin rumit ancamannya, dan menyoroti pentingnya manajemen resiko dan kerjasama dalam menghadapi ancaman siber[2].

Manajemen risiko siber dalam proyek-proyek teknologi informasi menjadi semakin penting untuk memastikan bahwa organisasi mampu mengidentifikasi, mengevaluasi, dan memitigasi ancaman yang dapat mengganggu pencapaian tujuan proyek[3], [4]. Proses ini tidak hanya melibatkan penerapan kontrol teknis, tetapi juga memerlukan pendekatan holistik yang mencakup kebijakan, prosedur, dan kesadaran pengguna[4].

Dengan demikian artikel ini bertujuan untuk memberikan tinjauan komprehensif tentang manajemen risiko siber dalam konteks proyek. Dimulai dengan identifikasi ancaman digital yang potensial, artikel ini akan mengeksplorasi berbagai metode evaluasi risiko yang digunakan untuk menilai tingkat ancaman tersebut. Selanjutnya, artikel ini akan membahas strategi mitigasi yang efektif untuk mengurangi risiko serta menyediakan studi kasus nyata yang menggambarkan penerapan manajemen risiko siber dalam proyek.

Untuk memuat projek, sebaiknya mempelajari manajemen resiko pada projek terlebih dahulu, sehingga dapat meminimalisir risiko dalam membuat projek tersebut . Resiko merupakan kejadian yang tidak diinginkan atau menyimpang dari tujuan awal dibuatnya suatu projek. Resiko ini muncul dikarenakan adanya ketidakpastian dari keputusan yang diambil. Karena resiko ada kejadian yang tidak diinginkan, kemungkinan besar resiko memiliki dampak buruk bagi projek tersebut. Untuk meminimilasir resiko ini, dapat dilakukan dengan memahami manajemen resiko. Manajemen resiko ini melibatkan pemantauan dan pengendalian resiko untuk memastikan bahwa resiko yang dikelola secara efektif pada projek. Hal ini penting dilakukan dalam menjalankan projek, karena dapat melindungi projek dari kerugian yang mungkin terjadi pada projek yang dilakukan.[6] Khususnya pada manajemen resiko *cyber crime*.

Cyber crime atau kejahatan didunia yang ada didunia maya merupakan salsh satu dampak negative yang muncul dari perkembangan teknologi informasi. Menurut OECD atau *Organization of European Community Development, cyber crime* merupakan suatu akses yang illegal didalam transmisi sebuah data. Salah satu aktivitas *cyber crime* adalah berupa pencurian data. Pencuarian data ini dapat berupa *hacking*, *cracking* dan yang lainnya [7].

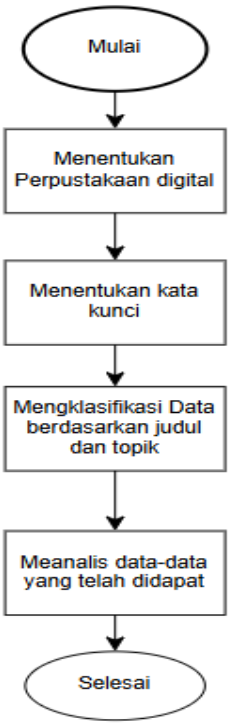
Dalam jurnal ini, terdapat sebuah studi kasus agar lebih mudah memahami bagaimana menerapkan manajemen resiko, yaitu tentang bagaimana cara Whatsapp menghadapi berbagai ancaman siber. Manajemen resiko apa saja yang diterapkan Whatsapp dengan fokus pada identifikasi, evaluasi, dan mitigasi ancaman digital. Dengan memahami dan menerapkan standar atau prinsip-prinsip manajemen resiko khususnya siber dengan baik, maka organisasi dapat lebih siap untuk menlewati tantangan yang ditimbulkan oleh lingkungan digital yang terus berubah[5]. Tinjauan ini akan memberikan wawasan dan panduan praktis bagi para manajer proyek dan profesional keamanan informasi dalam mengelola risiko siber dengan lebih efektif.

II. METODE PENELITIAN

Pada penelitian ini, metode yang digunakan adalah menggunakan studi literatur. Studi literatur sendiri melibatkan merangkum berbagai buku, artikel, jurnal serta dokumen-dokumen lain untuk memperoleh informasi tentang suatu topik yang diinginkan [8]. Studi literatur adalah penelitian yang telah dilakukan oleh peneliti sebelumnya. Studi literatur digunakan dengan mencari jurnal sebelumnya dengan judul yang berkaitan dengan topik yang mau dibahas Metode studi literatur ini penting bagi penelitian yang dilakukan ini untuk langkah awal pada perancangan penelitian dengan mengumpulkan data-data yang berkaitan dengan penelitian yang akan digunakan sebagai sumber data yang ada di perpustakaan online tanpa langsung mengumpulkan data di lapangan [9].

Karena metode Studi literatur yang digunakan adalah tinjauan literatur sehingga jurnal ini mengumpulakan data-data yang diperlukan yang sesuai dengan topik. Untuk mencari literatur yang berkaitan dengan topik yang telah ditentukan dari berbagai sumber online yang ada, baik itu jurnal dan artikel online serta berita yang ada pada situs surat kabar online. Dalam pemilihan jurnal ini, jurnal dan artikel didapat pada situs google scholar, sinta, garuda, dan ScieneDirect. Pemilihan sumber ini khususnya google scholar dikarenakan situs memiliki sifat yang open akses sehingga mudah untuk memperoleh data yang sesuai dengan topik. Kemudian mengidentifikasi kata kunci yang sesuai dengan topik yang dibahas seperti *cyber crime,* resiko keamanan informasi, mitigasi resiko *cyber,* evaluasi kebijakan keamanan, ancaman resiko dan manajemen resiko. Penentuan kata kunci ini mempermudah untuk mencari jurnal dan artikel yang relavan dengan topik yang dibahas. Proses pengambilan data yang digunakan dapat dilihat pada gambar 1.

Jurnal Manajemen Informatika (JAMIKA)
Volume 14 Nomor 2 Edisi Oktober 2024
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika



Gambar 1. *Flowchart* pengambilan data

Pertama, menentukan perpustakaan digital. Perpustakaan digital yang dipilih adalah google scholar, sinta, garuda, dan ScieneDirect. Dimana pada perpustakaan digital tersebut terdapat berbagai macam artikel dan jurnal. Artikel dan jurnal yang ada pada perpustakaan digital terdapat berbagai macam topik. Maka selanjutnya adalah menentukan kata kunci yang berkaitan dengan topik. Kata kunci yang digunakan adalah cyber crime, resiko keamanan informasi, mitigasi resiko cyber, evaluasi kebijakan keamanan, ancaman resiko dan manajemen resiko. Setelah memperoleh artikel dan jurnal dari perpustakaan digital berdasarkan kata kunci yang ditentukan, langkah selanjutnya adalah mengklasifikasi data yang didapat. Proses klasifikasi ini dilakukan berdasarkan judul dan topik dari artikel serta jurnal yang telah dikumpulkan. Proses ini dilakukan karena membantu mengorganisir dan mempermudah saat menganalis data. Langkah terakhir yang dilakukan adalah menganalisis data-data yang telah diklasifikasikan. Analis bertujuan untuk mendapatkan kesimpulan yang relavan dengan topik. Tabel 1 menunjukkan klasifikasi artikel yang telah didapat.

TABEL 1
KLASIFIKASI ARTIKEL

No	Judul Artikel	Topik		
		Ancaman	Evaluasi	Mitimigasi
1	Cyber crime di Indonesia cyber crime information and communication technology crime risks and innovation analysis of cyber crime risk prevention in indonesia	✓	✓	
2	Degradasi moral sebagai dampak kejahatan siber pada generasi millenial di Indonesia	✓		
4	Jenis peningkatan keamanan cyber: studi kasus ancaman dan solusi dalam lingkungan	✓	✓	

Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume 14 Nomor 2 Edisi Oktober 2024
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

No	Judul Artikel	Topik		
		Ancaman	Evaluasi	Mitimigasi
	digital untuk mengamankan objek vital dan file			
5	Mengenal hacking sebagai salah satu kejahatan di dunia maya	✓		
6	Kajian normatif penanganan cyber crime di sektor perbankan di Indonesia	✓	✓	
7	Perlindungan hukum terhadap korban pada kasus cyber sabotage and extortation menurut hukum positif di Indonesia	✓	✓	
8	Carding crime as a form of cyber crime in Indonesian criminal law	✓		
9	Indeks keamanan siber Indonesia peringkat ke-3 terendah di antara negara g20		✓	
10	Ancaman cybercrime di Indonesia: sebuah tinjauan pustaka sistemati	✓	✓	✓
11	Pendampingan analisis vulnerability dan hardening pada website pemerintah kota Surabaya	✓	✓	
12	Thoughts on the potential threat of cyber war in Indonesia: a defense strategy study	✓	✓	
13	Pengenalan pentingnya cyber security awareness pada umkm		✓	✓
14	Analis manjemen resiko keamanan informasi menggunakan nist cybersecurity framework dan ISO/IEC	✓	✓	
15	Cybersecurity strategy for smart city implementation	✓	✓	✓
16	Data and information security management: preparing data in the cyber era in Indonesia	✓	✓	✓
17	Ransomware: memahami ancaman kemanan digital	✓		
18	Analisis evaluasi kebijakan pada cyber security perbankan	✓	✓	
19	Penerapan kebijakan digital dalam rangka pencegahan cyber crime		✓	✓
20	Penguatan manajemen risiko lembaga keuangan syariah non-bank dalam menghadapi ancaman cyber security		✓	

Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume 14 Nomor 2 Edisi Oktober 2024
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

No	Judul Artikel	Topik		
		Ancaman	Evaluasi	Mitimigasi
21	Mitigasi risiko: analisis terhadap antisipasi resiko dalam pembiayan mikro syariah	✓	✓	✓
22	Risiko dan mitigasi penggunaan kecerdasan buatan dalam bidang pendidikan	✓	✓	✓
23	Strategi mitigasi resiko keamanan informasi berdasarkan analisa return on investment pada badan pusat statistik daerah kota Semarang	✓	✓	✓

Pada tabel 1 didapatkan 23 artikel. Artikel-artikel ini dikelompokan berdasarkan tiga topik utama, yaitu dari mengidentifikasi ancaman, evaluasi sisten keamanan, hingga strategi mitigasi. Artikel ini didapatkan dengan menggunakan kata kunci cyber crime, resiko keamanan informasi, mitigasi resiko cyber, evaluasi kebijakan keamanan, ancaman resiko dan manajemen resiko. Dari banyaknya artikel tersebut, sebanyak 16 artikel yang didapat membahas tentang identifikasi bentuk ancaman siber, artikel tersebut memberikan informasi tentang jenis kejahatan siber dan dampaknya, Dan juga sebanyak 15 artikel yang membahas evaluasi, yang membahas tentang pentingnya penilaian keamanan siber yang ada, dengan menilai kerangka kerja dan kebijakan yang ada. Terdapat pula, 14 artikel yang membahas mitigasi, yang menjelaskan tentang metode untuk mengurangi ressiko dan meningkatkan kemanan informasi, misalnya dengan cara mengunkan metode untuk mengidentifikasi potensi dan ancaman, yaitu dengn cara menilai resiko, menilai kerentanan sistem. mengumpulkan data intelejen, mengidentifikasi aset dan ancaman. Secara keseluruhan, ketiga jenis artikel ini memberikan pandangan menyeluruh tentang keamanan siber.

Setelah mengklasifikasi artikel yang didapat, selanjutnya menganalis data-data yang didapat. Dengan cara membaca artikel secara keseluruhan dan mendapatkan ringkasan dari artikel yang telah dibaca. Ringkasan yang berisi informasi itu, akan dijadikan kalimat-kalimat yang mudah dibaca dan dipahami.

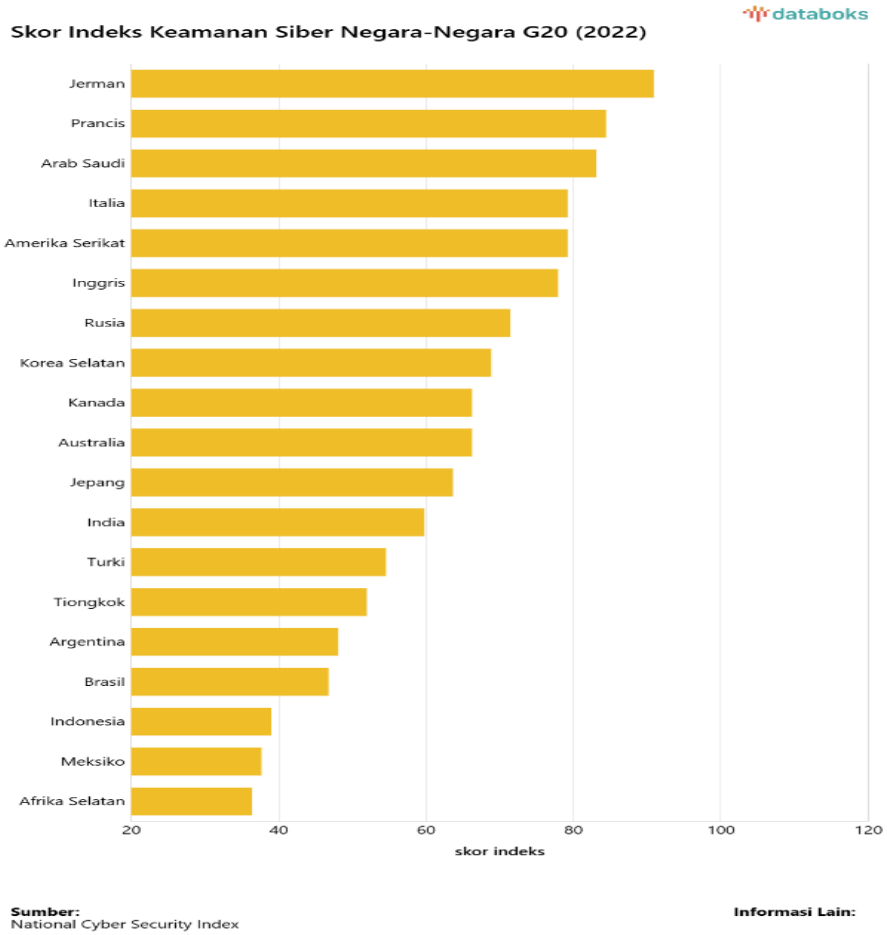
III. HASIL DAN PEMBAHASAN

Dari pesatnya perkembangan teknologi yang terjadi menyebabkan munculnya dampak *cyber* yang bermunculan baik itu dampak positif maupun negative[10]. Dengan terjadinya tingkatan pemanfaat pada ruang siber (*cyberspace*) dalam kehidupan sehari-hari terdapat kejahatan yang muncul sebagai dampak negative dari perkembangan teknologi yang disebut kejahatan siber (*cyber crime*) [11]. *Cybercrime* sendiri adalah permasalahan yang muncul dengan menggunakan komputer dengan bebas atau illegal untuk memperoleh keuntungan dan merugikan pihak lain, sehingga menjadi perbuatan yang melawan hukum[12].

Perlu diketahui pula, terdapat beberapa jenis *cybercrime* yang terjadi, yang pertama *hacking* adalah aktivitas memasuki sistem komputer milik orang atau organisasi lain tanpa izin dari pemillik, yang melakukan aktivitas ini biasanya adalah *hacker*. *Hacker* akan mengotak-atik komputer, dan mengamati keamanan *security* nya, lalu menerobos program yang ada pada komputer tersebut untuk merusak atau mencuri data yang ada[13], [14] Selanjutnya, *cracking* adalah bentuk *hacking* yang memiliki tujuan kejahatan. Yang melakukan *cracking* biasa adalah *hacker* bertopi hitam atau bisa disebut dengan *cracker*. *Cracker* akan mengakses program yang ada pada komputer dan mengambil data-data yang sensitive demi keuntungan pribadi [13], [15]. Lalu ada pula *cyber* sabotage, yaitu kejahatan dengan menghancurkan data, menghancurkan sistem program yang menjalankan komputer dan juga menghancurkan sistem jaringan pada komputer yang terhubung dengan internet. Hal ini bisa terjadi karena pelaku memasukan virus komputer pada program, hingga data pada komputer tersebut tidak berjalan dengan semestinya atau rusak[13], [16]. Selanjutnya ada *cyber attack*, yaitu semua kegiatan yang dengan sengaja menganggu kerahasian, integritas dan ketersedian informasi [13], [14]. Dan adapula, yaitu kejahatan yang menggunakan identitas atau kartu kredit orang lain, yaitu *carding*. *Carding* ini adalah aktvitas dengan berbelanja menggunakan kartu kredit orang lain yang didapat secara illegal, biasanya dilakukan dengan mengambil data di internet[14], [17]. Dan terakhir adalah *spyware*, yaitu kegiatan merekam suatu aktivitas online secara rahasia atau tidak diketahui oleh yang bersangkut, hal yang direkam biasanya adalah *cookies* atau *registry*. Data yang telah direkam akan dikirimkan atau dijual pada orang atau organisai yang akan mengirimkan iklan dan menyebarkan virus[14].

Jurnal Manajemen Informatika (JAMIKA)
Volume 14 Nomor 2 Edisi Oktober 2024
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Dilansir dari website databoks, menurut laporan *national cyber security index* atau disingkat NCSI, Indonesia memuliki skor indeks sebesar 38.96 di tahun 2022. Dengan skor indeks sebesar itu menempatkan Indonesia pada peringkat terendah ke-tiga di antara negara-negara G20[18].



Gambar 1. Indeks kemanan siber negara G20[18]

Jadi alangkah baiknya, sebelum melakukan sebuah project seharusnya melakukan kegiatan yang dapat mengidentifikasi *cyber security* agar dapat mengurangi resiko projek diserang[19] Terdapat metode identifikasi *cyber security* sendiri melibatkan beberapa langkah yang efektif untuk mengidentifikasi potensi ancaman dan risiko. Berikut adalah beberapa metode identifikasi potensi ancaman dan resiko yang dapat digunakan:

Penilaian Risiko

Penilaian risiko adalah proses sistematis untuk memahami sifat dan tingkat risiko yang dapat mengganggu operasi bisnis. Dalam konteks ancaman siber, ini melibatkan:

1) Analisis SWOT: Analisis kekuatan, kelemahan, peluang, dan ancaman dalam infrastruktur IT. Ini membantu mengidentifikasi di mana potensi ancaman dan kerentanan mungkin muncul dan bagaimana mereka dapat dieksploitasi.
2) Analisis Skenario: Mengembangkan skenario berbasis ancaman yang mungkin terjadi. Ini mencakup peristiwa seperti serangan *malware*, *phishing*, dan serangan *denial-of-service* (DoS).
3) Pendekatan Berbasis Ancaman: Fokus pada ancaman spesifik yang dapat mempengaruhi organisasi berdasarkan intelijen ancaman yang ada. Ini membantu dalam mengidentifikasi vektor serangan potensial dan merancang strategi mitigasi.

Penilaian Kerentanan

Penilaian kerentanan merupakan sebuah proses untuk mencari menilai tingkat keparahan, dan menentukan prioritas kelemahan yang terdapat pada sistem serta jaringan komputer:

1) Scan Kerentanan: Menggunakan alat-alat otomatis seperti Nessus, OpenVAS, atau Qualys untuk memindai sistem dan jaringan terhadap kerentanan yang dikenal.
2) Audit Keamanan: Melakukan audit manual dan otomatis untuk memastikan bahwa kontrol keamanan telah diterapkan dengan benar dan berfungsi sesuai yang diharapkan.
3) *Penetration Testing* (Pentest): Simulasi serangan siber untuk menemukan titik lemah yang bisa dieksploitasi oleh penyerang.

Pengumpulan Data Intelijen

Pengumpulan data intelijen bertujuan untuk mendapatkan informasi tentang ancaman yang sedang berkembang dan teknik serangan terbaru:

1) *Threat Intelligence*: Melibatkan pengumpulan dan analisis informasi dari berbagai sumber seperti laporan keamanan siber, basis data ancaman, dan komunitas keamanan untuk memahami ancaman terbaru dan pola serangan.
2) Monitoring Media Sosial: Mengamati aktivitas di media sosial dan forum-forum khusus yang mungkin mengungkap rencana serangan atau teknik baru yang sedang dibahas oleh penyerang.
3) *Feed Threat Intelligence*: Mengintegrasikan *feed* intelijen ancaman yang terus diperbarui ke dalam sistem keamanan untuk deteksi dini dan respons cepat.

Identifikasi Aset

Identifikasi aset adalah proses mengenali dan mengklasifikasikan aset-aset penting dalam organisasi yang perlu dilindungi, seperti sistem informasi, jaringan, dan perangkat keras, serta mengklasifikasikan mereka berdasarkan kategori risiko dan prioritas:

1) Katalog Aset: Membuat daftar semua aset IT seperti server, perangkat jaringan, aplikasi, dan data penting.
2) Klasifikasi Aset: Menentukan nilai dan sensitivitas setiap aset untuk mengarahkan upaya perlindungan sesuai dengan prioritas.
3) *Criticality Analysis*: Menilai aset berdasarkan pentingnya terhadap operasi bisnis dan potensi dampak jika aset tersebut dikompromikan.

Identifikasi Ancaman

Identifikasi ancaman melibatkan mengidentifikasi potensi ancaman yang dapat mengeksploitasi kerentanan dalam sistem, seperti serangan siber, virus, Trojan, dan perubahan data:

1) *Threat Modeling*: Membuat model yang menggambarkan bagaimana ancaman dapat berinteraksi dengan sistem, termasuk vektor serangan dan kemungkinan dampaknya.
2) Analisis Historis: Melihat insiden keamanan masa lalu untuk mengidentifikasi pola dan tren yang dapat menunjukkan ancaman masa depan.
3) *Expert Consultation*: Berkonsultasi dengan pakar keamanan siber dan menggunakan metode Delphi untuk mendapatkan pandangan yang beragam tentang ancaman yang mungkin dihadapi.

Perkembangan teknologi digital telah meningkatkan ancaman *cybercrime* secara signifikan[20]. Dampak dari *cyber* ini dapat mengubah kehidupan masyarakat, termasuk sektor ekonomi, bisnis, politik dan budaya, menjadi semakin terikat dengan teknologi [21]. Oleh karena itu, penting bagi suatu proyek untuk memahami dampak dari resiko *cyber* yang ada. Selain dampak positif, ada pula dampak negative yang di dapat[22]. Tak jarang pula dampak yang didapat membuat kerugian finansial bagi organisasi, gangguan operasional, kehilangan data dan informasi serta memperngaruhi reputasi dan kepercayaan pemangku kepentingan [21], [23].

Karena semakin banyaknya serangan *cyber* yang ada dan semakin sulit terditeksi, maka dari itu suatu proyek harus mengetahui penilaian dampak resiko serangam *cyber* ini[24] Dengan cara mehami resiko-resiko dan ancaman-ancaman *cyber*, mengembangkan strategi untuk menangani ancaman *cyber*, dan mempersiapkan infrastruktur, sumber daya, dan kemampuan untuk mengahadapi resiko *Cyber*[25], [26].

Pada jurnal dengan judul "Model implementas Mission Assurance dalam Business Process Management", dikatakan bahwa metode evaluasi untuk resiko *cyber* adalah menganalis evaluasi kebijakan *cybersecurity* yang dimiliki, dan juga mengevaluasi teknologi keamanan informasi yang dipilih dan diterapkan, karena pada setiap teknologi pasti memiliki kesempatan bagi pelaku kejahatan *cyber* untuk beraksi. Dan terakhir, analisis upaya pencegahan yang dilakukan untuk meminimalkan resiko dan dampak kejahatan *cyber*[27].

Jurnal Manajemen Informatika (JAMIKA)
Volume 14 Nomor 2 Edisi Oktober 2024
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Pencegahan yang dapat dilakukan antara lain, memiliki kebijakan dan prosedur yang memadai untuk penggunaan teknologi informasi, di indonesia sendiri terdapat tim khusus untuk memantau dan memberantas *cybercrime* dan juga terdapat undang-undang yang diterapkan untuk kasus-kasus *cybercrime* [28], [29]. Selain itu, dapat melalukan identifikasi, pengukuran, pengendalian, dan pemantauan resiko tekonologi informasi yang memandai [29].

Mitigasi resiko ancaman *cyber* ini dilakukan untuk mencari solusi atas konsekuensi yang merugikan proyek . Mitigasi biasanya memunculkan aturan atau kebijakan untuk mengurangi atau menghalangi kerugian yang mungkin terjadi [30]. Mitigasi dapat dilakukan dengan memastikan keamanan perangkat, dengan menjaga perangkat yang digunakan[31]. Lalu mengidentifikasi asset informasi utama, menentukan faktor paparan yang memperkirakan persentase kerugian, dan setelahnya melakukan pendekatan keseluruhan untuk mengidentifikasi ancaman, potensi kerugian, dan mengevaluasi tindakan yang tepat [32].

Salah satu studi kasus yang diteliti adalah WhatsApp. WhatsApp adalah aplikasi komunikasi yang banyak digunakan, aplikasi ini tak luput menghadapi berbagai ancaman siber. Studi kasus ini akan mengkaji bagaimana manajemen risiko siber diterapkan pada WhatsApp dengan fokus pada identifikasi, evaluasi, dan mitigasi ancaman digital.

Identifikasi Ancaman

Beberapa metode atau langkah yang dapat mengidetifikasi ancaman dalam aplikasi WhatsApp, yaitu:

1) Analisis Kerentanan
   Melakukan pemeriksaan aplikasi secara rutin untuk menemukan kerentanan atau bug yang dimanfaatkan oleh pelaku. Ini termasuk pengujian penetrasi dan analisis kode sumber.
2) Monitoring dan Logging
   Memantau aktivitas jaringan dan mencatat log aplikasi untuk mendeteksi aktivitas yang mencurigakan atau tidak biasa yang mungkin menunjukkan adanya ancaman keamanan.
3) Analisis Ancaman (*Threat Analysis*)
   Melakukan analisis yang mendalam terhadap potensi ancaman yang mungkin dihadapi aplikasi, termasuk dalam menganalisis teknik dan taktik yang dilakukan oleh pelaku kejahatan.
4) Penilaian Risiko (*Risk Assessment*)
   Menilai risiko yang terkait dengan setiap ancaman yang teridentifikasi, termasuk potensi dampak dan kemungkinan terjadinya. Ini membantu dalam memprioritaskan ancaman dan mengembangkan strategi mitigasi.
5) Tes Penetrasi *(Penetration Testing*)
   Melibatkan penggunaan teknik yang digunakan oleh penyerang untuk mencoba menembus sistem keamanan aplikasi. Ini membantu dalam mengidentifikasi dan memperbaiki kelemahan sebelum dieksploitasi oleh penyerang.
6) Simulasi Serangan (*Red Teaming*)
   Tim yang bertugas untuk melakukan simulasi serangan siber dengan tujuan menguji keamanan sistem dan kesiapan tim respons.
7) Pengumpulan Intelijen Ancaman (*Threat Intelligence*)
   Mengumpulkan informasi dari berbagai sumber mengenai ancaman yang sedang tren dan teknik yang digunakan oleh pelaku untuk tetap waspada terhadap ancaman yang muncul.
8) Pendidikan dan Pelatihan Pengguna
   Mengadakan program pelatihan dan kesadaran keamanan untuk pengguna akhir guna mengurangi risiko serangan yang memanfaatkan kesalahan manusia, seperti serangan phishing.

Evaluasi Risiko

Evaluasi risiko meliputi identifikasi risiko dan penilaian risiko. Berikut ini paparan identifikasi dan penilaian risiko yang berkaitan dengan WhatsApp:

1) Identifikasi Risiko
   Mengidentifikasi berbagai ancaman dan kerentanan yang dapat mempengaruhi WhatsApp dan penggunanya:
   a. Phishing: Usaha untuk menipu pengguna agar memberikan informasi sensitif, seperti kode verifikasi atau detail login.
   b. Serangan Man-in-the-Middle (MitM): Ancaman yang mencoba mengintersepsi komunikasi antara pengguna.
   c. Pengambilalihan Akun: Akses tidak sah ke akun pengguna yang dapat menyebabkan pencurian identitas dan data.

2) Penilaian Risiko
Evaluasi risiko melibatkan analisis dampak, kemungkinan, dan kategori dari setiap ancaman yang telah diidentifikasi. Tabel 2 menunjukkan matrik risiko, seperti phising, serangan MitM, dan pengambilan akun serta dampak, kemungkinan dan kategorinya.

TABEL 2
MATRIKS RISIKO

Risiko	Dampak	Kemungkinan	Kategori
Phishing	Tinggi	Sedang	Menengah
Serangan MitM	Sangat tinggi	Rendah	Rendah
Pengambilalihan Akun	Tinggi	Sedang	Menengah

a. Phishing
Dampak: Tinggi (pencurian data sensitif, akses akun pengguna, penyebaran malware).
Kemungkinan: Sedang (berdasarkan frekuensi laporan insiden).
Kategori: Menengah, karena kombinasi dari dampak tinggi dan kemungkinan sedang menempatkan risiko ini dalam kategori menengah, menunjukkan perlunya perhatian serius namun tidak kritis.
Mitigasi: Edukasi pengguna tentang tanda-tanda phishing, fitur verifikasi dua langkah (2FA).
b. Serangan Man-in-the-Middle (MitM)
Dampak: Sangat tinggi (pengungkapan komunikasi pribadi).
Kemungkinan: Rendah (karena adanya enkripsi end-to-end yang secara signifikan mengurangi risiko ini).
Kategori: Rendah, jadi meski dampaknya besar, rendahnya kemungkinan terjadinya serangan ini menempatkannya dalam kategori risiko rendah.
Mitigasi: Terus meningkatkan protokol enkripsi dan melakukan audit keamanan secara berkala.
c. Pengambilalihan Akun
Dampak: Tinggi (kontrol penuh atas akun pengguna, potensi penyalahgunaan data).
Kemungkinan: Sedang (bisa terjadi melalui berbagai metode seperti social engineering).
Kategori: Menengah, seperti pada phishing, risiko ini dikategorikan sebagai menengah karena dampaknya yang tinggi dan kemungkinan sedang.
Mitigasi: Implementasi patching dan update reguler, penggunaan 2FA, dan deteksi aktivitas mencurigakan.

Adapun langkah-langkah yang dapat dilakukan untuk mencegah serangan phishing online, contohnya seperti:

a. Meningkatkan kesadaran organisasi terhadap ancaman dunia maya.
b. Menerapkan standar keamanan jaringan informasi di seluruh organisasi.
c. Melatih sumber daya manusia untuk menjaga keterampilan keamanan siber.
d. Menerapkan dan memperbarui arsitektur sistem dan layanan yang aman secara berkala.
e. Potensi untuk pencegahan, mitigasi, koreksi dan revisi. [4]

Untuk mencegah serangan MitM dapat dilakukan dengan memastikan komunikasi selalu terenkripsi dan selalu melakukan audit keamanan secara berkala untuk mengidentifikasi dan memperbaiki kerentanan. Sedangkan untuk Pengambilalihan Akun dapat dengan memastikan semua perangkat lunak diperbarui secara berkala untuk memperbaiki kerentanan serta menggunakan algoritma untuk mendeteksi dan merespon aktivitas yang mencurigakan.

Strategi Mitigasi

Berikut ini strategi mitigasi yang dapat dilakukan, yaitu:

1) Keamanan Aplikasi:
a. *Enkripsi End-to-End*: Di mana semua pesan dan panggilan WhatsApp di*enkripsi*, sehingga yang dapat membaca pesan hanya pengirim dan penerima, karena itu pengguna mamiliki privasi yang lebih ketat.
b. Verifikasi Dua Langkah: Pengguna diminta memasukkan PIN tambahan saat mengakses akun dari perangkat baru.

c. *Patch* dan Pembaruan: WhatsApp secara rutin memperbarui aplikasi untuk menambal kerentanan keamanan.

2) Kesadaran dan Pendidikan Pengguna:
   a. Kampanye Kesadaran: Mengedukasi pengguna tentang bahaya *phishing*, *social engineering*, dan pentingnya verifikasi dua langkah.
   b. Peringatan dan Notifikasi: Memberikan notifikasi ketika aktivitas mencurigakan terdeteksi, seperti login dari perangkat baru.
3) Pemantauan dan Deteksi:
   a. Sistem Deteksi Intrusi: Menggunakan algoritma deteksi untuk mengidentifikasi pola perilaku mencurigakan.
   b. Pemantauan *Real-Time*: Memantau lalu lintas jaringan dan aktivitas pengguna secara *real-time* untuk mendeteksi dan merespons ancaman dengan cepat.

IV. KESIMPULAN

Manajemen risiko siber dalam konteks proyek sangat krusial bagi organisasi untuk melindungi data dan aset serta memastikan kelangsungan dan kesuksesan proyek di tengah lingkungan digital yang semakin kompleks dan penuh tantangan. Proses ini melibatkan identifikasi ancaman digital potensial seperti hacking, cracking, cyber sabotage, spyware, carding, dan berbagai bentuk serangan malware. Evaluasi risiko mencakup penilaian dampak negatif dan positif dari ancaman tersebut. Strategi mitigasi ancaman diterapkan untuk mengurangi atau mencegah kerugian. Penelitian selanjutnya difokuskan pada pengembangan teknologi deteksi dan respon ancaman yang lebih canggih, seperti penggunaan kecerdasan buatan, serta evaluasi efektivitas strategi mitigasi yang ada dan pengembangan program pelatihan keamanan siber. Integrasi manajemen risiko siber dengan manajemen proyek secara keseluruhan dan kepatuhan terhadap regulasi keamanan yang terus berkembang sangat penting. Studi kasus WhatsApp menunjukkan bahwa strategi manajemen risiko siber yang efektif dapat meningkatkan keamanan platform dan kepercayaan pengguna, meskipun ancaman seperti phishing, malware, dan serangan man-in-the-middle tetap ada. Langkah-langkah yang telah diambil WhatsApp, termasuk enkripsi end-to-end, pembaruan keamanan berkala, dan edukasi pengguna, telah cukup efektif, namun masih diperlukan peningkatan teknologi deteksi dan respon serta relevansi kebijakan dan praktik keamanan.

DAFTAR PUSTAKA

[1] A. Frisdayanti, "PERANAN BRAINWARE DALAM SISTEM INFORMASI MANAJEMEN," vol. 1, 2019, doi: 10.31933/JEMSI. Available: JEMSI (Jurnal Ekonomi, Manajemen, dan Akuntansi) (lembagakita.org) [Accessed: 23-May-2024]

[2] A. Bustami and S. Bahri, "Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review," 2020. Available: Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review | UNISTEK [Accessed: 23-May-2024]

[3] Rahamadanis, Rani Novita, Reka Zulihanifa Wati, and Reni Mardiana, "Efektivitas Penerapan Manajemen Resiko Pada PT. Indofood Sukses Makmur," *Jurnal Magisma*, vol. 11, no. 2, pp. 163–172, 2023. Available: Efektivitas Penerapan Manajemen Risiko Pada PT. Indofood Sukses Makmur | Magisma: Jurnal Ilmiah Ekonomi dan Bisnis (stiebankbpdjateng.ac.id) [Accessed: 23-May-2024]

[4] R. Kuswulandari, A. Wirid, I. Jowanka, T. Nabila, P. Riyanto, and T. Listiani, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp," 2023. Available: Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Aplikasi Whatsapp | Prosiding Seminar Nasional Teknologi Informasi dan Bisnis (udb.ac.id) [Accessed: 23-May-2024]

[5] Yohanes Ngamal, "PENERAPAN MODEL MANAJEMEN RISIKO TEKNOLOGI DIGITAL DI LEMBAGA PERBANKAN BERKACA PADA CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN INDONESIA," 2022. [Online]. Available: www.ojk.go.id [Accessed:23-May-2024]

[6] Ferdinandus Sampe *et al.*, *Manajemen Risiko*. Banten: PENERBIT PT SADA KURNIA PUSTAKA, 2023. [Accessed: 25-May-2024]

[7] N. Widya Ramailis, "CYBER CRIME DAN POTENSI MUNCULNYA VIKTIMISASI PEREMPUAN DI ERA TEKNOLOGI INDUSTRI 4.0," 2020. [Online]. Available: https://qwords.com/ Available: [Accessed: 27-May-2024]

[8] M. A. Faturrahman and K. Ningsih, "Studi Literatur: Penerapan Model Discovery Learning terhadap Hasil Belajar Peserta Didik pada Materi Klasifikasi Makhluk Hidup," *Journal on Education*, vol. 6,

no. 1, pp. 7262–7274, Jul. 2023, doi: 10.31004/joe.v6i1.3956. Available: Studi Literatur: Penerapan Model Discovery Learning terhadap Hasil Belajar Peserta Didik pada Materi Klasifikasi Makhluk Hidup | Semantic Scholar [Accessed: 28-May-2024]

[9] N. E. Nurjanah and T. T. Mukarromah, "Pembelajaran Berbasis Media Digital Pada Anak Usia Dini Di Era Revolusi Industri 4.0 : Studi Literatur," *Jurnal Ilmiah Potensia*, vol. 6, no. 1, pp. 66–77, 2021, doi: 10.33369/jip.6.1. Available: Pembelajaran Berbasis Media Digital pada Anak Usia Dini di Era Revolusi Industri 4.0 : Studi Literatur - Neliti [Accessed: 26-May-2024]

[10] N. Maharani Harahap and U. Islam Negeri Sumatera Utara, "CYBER CRIME DI INDONESIA CYBER CRIME INFORMATION AND COMMUNICATION TECHNOLOGY CRIME RISKS AND INNOVATION ANALYSIS OF CYBER CRIME RISK PREVENTION IN INDONESIA," *Jurnal Teknologi dan Manajemen Sistem Industri (JTMSI)*, vol. 3, no. 1, p. 2024. Available: https://ojs.ejournalunigoro.com/index.php [Accessed:27-May-2024]

[11] T. Heru, D. Wijaya, and N. Sahputra Umara, "Degradasi Moral sebagai Dampak Kejahatan Siber pada Generasi Millenial di Indonesia," 2022. [Accessed: 29-May-2024]

[12] Nurbaiti Mu'rufah, Hayatul Khairul Rahmat, and I Dewa Ketut Kerta Widana, "DEGRADASI MORAL SEBAGAI DAMPAK KEJAHATAN SIBER PADA GENERASI MILLENIAL DI INDONESIA," *Tahun*, vol. 7, no. 1, pp. 191–201, 2020, doi: 10.31604/jips.v7i1.2020.191-201. Available: DEGRADASI MORAL SEBAGAI DAMPAK KEJAHATAN SIBER PADA GENERASI MILLENIAL DI INDONESIA | Marufah | NUSANTARA : Jurnal Ilmu Pengetahuan Sosial (um-tapsel.ac.id) [Accessed: 28-May-2024]

[13] Edy Soesanto, Achamd Romadhon, Bima Dwi Mardika, and Moch Fahmi Setiawan, "Analis dan Peningkatan Kemanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File," *SAMMAJIVA: Jurnal Penelitian Bisnis dan Manajemen*, pp. 172–191, 2023. Available: Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File | Sammajiva: Jurnal Penelitian Bisnis dan Manajemen (nalanda.ac.id) [Accessed: 28-May-2024]

[14] Sari Indah, "MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN DI DUNIA MAYA," 2023. Available: MENGENAL HACKING SEBAGAI SALAH SATU KEJAHATAN DI DUNIA MAYA | Sari | JSI (Jurnal sistem Informasi) Universitas Suryadarma [Accessed:-May-2024]

[15] A. Alhakim, "KAJIAN NORMATIF PENANGANAN CYBER CRIME DI SEKTOR PERBANKAN DI INDONESIA," 2021. Available: KAJIAN NORMATIF PENANGANAN CYBER CRIME DI SEKTOR PERBANKAN DI INDONESIA | Jurnal Komunitas Yustisia (undiksha.ac.id) [Accessed: 28-May-2024]

[16] D. Ayuna Letri and T. Rahmi Gettari, "PERLINDUNGAN HUKUM TERHADAP KORBAN PADA KASUS CYBER SABOTAGE AND EXTORTATION MENURUT HUKUM POSITIF DI INDONESIA," vol. 2, doi: 10.36355/.v1i2. Available: https://ojs.umb-bungo.ac.id/index.php [Accessed: 25-May-2024]

[17] O. Kaimuddin Haris, S. Hidayat, and R. Dwitasari, "Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia Carding Crime as a Form of Cyber Crime in Indonesian Criminal Law," 2023. [Online]. Available: https://www.hukumonline.com/klinik/a/tindak-pidana-cyber-crime-cl2824/. [Accessed: 26 -May-2024]

[18] Cindy Mutia Annur, "Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20," databoks. Available: https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20 [Accessed: 27-May-2024]

[19] B. Setiawan, F. Samopa, I. A. Akbar, N. A. Sani, B. C. Hidayanto, and Y. S. Dharmawan, "Pendampingan Analisis Vulnerability dan Hardening pada Website Pemerintah Kota Surabaya," *Sewagati*, vol. 7, no. 6, pp. 897–906, Oct. 2023, doi: 10.12962/j26139960.v7i6.624. Available: [PDF] Pendampingan Analisis Vulnerability dan Hardening pada Website Pemerintah Kota Surabaya | Semantic Scholar [Accessed: 27-May-2024]

[20] R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *Jurnal Konstituen*, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208. Available: https://ejournal.ipdn.ac.id/konstituen/article/view/3208 [Accessed: 28-May-2024]

[21] B. A. Darumaya, S. Maarif, T. Toruan, Y. Swastanto, P. Doktoral, and F. Strategi, "Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan Thoughts on the Potential Threat of Cyber War in Indonesia: a Defense Strategy Study," vol. IX, no. 2, pp. 299–324, 2023.[Accessed: 28-May-2024]

[22] I. Made Suartana, R. E. Putra, R. Bisma, and A. Prapanca, "PENGENALAN PENTINGNYA CYBER SECURITY AWARENESS PADA UMKM," 2022. [Online]. Available: http://jurnal.unipasby.ac.id/index.php/abadimas [Accessed: 27-May-2024]

[23] Tasha Safira Putri, Nurul Mutiah, and Dian Prawira, "Analis Manjemen Resiko Keamanan Informasi Menggunakan NIST CyberSecurity Framework dan ISO/IEC," 2022. Available: https://jurnal.untan.ac.id/index.php/jcskommipa/article/view/54972 [Accessed: 26-May-2024]

[24] R. G. G. Alam and H. Ibrahim, "Cybersecurity Strategy for Smart City Implementation," in *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences - ISPRS Archives*, International Society for Photogrammetry and Remote Sensing, Sep. 2019, pp. 3–6. doi: 10.5194/isprs-archives-XLII-4-W17-3-2019. Available: https://isprs-archives.copernicus.org/articles/XLII-4-W17/3/2019/ [Accessed: 25-May-2024]

[25] R. A. Hajj, A. Muta'ali, and B. J. Mamoto, "Data and Information Security Management: Preparing Data in the Cyber Era in Indonesia," *Budapest International Research and Critics Instititute-Journal* , vol. 5, no. 3, pp. 19165–19171, 2022, doi: 10.33258/birci.v5i3.5924. Available: https://scholar.ui.ac.id/en/publications/data-and-information-security-management-preparing-data-in-the-cy [Accessed: 25-May-2024]

[26] Budi Hartono, "Ransomware: Memahami Ancaman Kemanan Digital," *Bincang Sains dan Teknologi (BST)*, vol. 2, no. 02, pp. 55–63, 2023. Available: https://journal.iistr.org/index.php/BST/article/view/353 [Accessed: 25-May-2024]

[27] D. Chirzah and Y. Al-Fadli, "ANALISIS EVALUASI KEBIJAKAN PADA CYBER SECURITY PERBANKAN," 2023. Available: https://karya.brin.go.id/id/eprint/17937/ [Accessed:-May-2024]

[28] R. Sari br Sembiring, V. Saputra Ginting, E. Benna Perolihin Manurung, J. Simanullang, and K. Kunci, "PENERAPAN KEBIJAKAN DIGITAL DALAM RANGKA PENCEGAHAN CYBER CRIME." [Online]. Available: https://journal-mandiracendikia.com/index.php/pkm [Accessed: 26-May-2024]

[29] F. A. Kurniawan and K. Solihin, "Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security," *JIOSE: Journal of Indonesian Sharia Economics*, vol. 1, no. 1, pp. 1–20, Mar. 2022, doi: 10.35878/jiose.v1i1.360. Available: https://karya.brin.go.id/id/eprint/17937/ [Accessed: 28-May-2024]

[30] POPI ADIYES PUTRA, SAPARUDDIN, and NURNASRINA, "MITIGASI RISIKO: ANALISIS TERHADAP ANTISIPASI RESIKO DALAM PEMBIAYAN MIKRO SYARIAH.," 2023. Available: https://ejournal.uinib.ac.id/febi/index.php/almasraf/article/viewFile/414/pdf [Accessed: 27-May-2024]

[31] Aji Cokro Dewanto, "RISIKO DAN MITIGASI PENGGUNAAN KECERDASAN BUATAN DALAM BIDANG PENDIDIKAN," *Prosiding Konferensi Ilmiah Pendidikan*, vol. 4, pp. 1–10, 2023. Available: https://proceeding.unikal.ac.id/index.php/kip/issue/view/22 [Accessed: 28-May-2024]

[32] A. Rohmani and M. Gunawan Wibisono, "STRATEGI MITIGASI RESIKO KEAMANAN INFORMASI BERDASARKAN ANALISA RETURN ON INVESTMENT PADA BADAN PUSAT STATISTIK DAERAH KOTA SEMARANG," 2020. Available https://core.ac.uk/outputs/88049933/: [Accessed: 27-May-2024]