**Journal of Applied Informatics and Computing (JAIC)**
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861 

# Analisis Perilaku Mahasiswi Politeknik Negeri Batam Dalam Menanggapi Ancaman Digital Berdasarkan Pilar *Respond* dan *Recover* Menurut *NIST Framework*

**Lisa Rahma Putri [1*], Hamdani Arif [2**]**
*Rekayasa Keamanan Siber, Politeknik Negeri Batam
**Rekayasa Keamanan Siber, Politeknik Negeri Batam
lisaputri1202@gmail.com [1], hamdaniarif@polibatam.ac.id [2]

**Article Info**

***Article history:***

Received …
Revised …
Accepted …

***Keyword:***

*Cybersecurity, Students, NIST, Digital Recovery, Security Behavior, Incident Response.*

**ABSTRACT**

*The advancement of digital technology has increased the risk of information security threats, particularly for university students who are active internet users in academic and social activities. This study aims to analyze the behavior of students at Politeknik Negeri Batam in responding to and recovering from digital incidents, based on two pillars of the NIST Cybersecurity Framework: Respond and Recover. A descriptive quantitative approach was used through a survey method. Data were collected via an online questionnaire distributed to active students and analyzed using descriptive statistics along with validity and reliability tests. The results of this study are expected to provide a comprehensive overview of students' cybersecurity literacy and serve as a foundation for developing educational strategies and digital security policies within higher education institutions.*



## I. PENDAHULUAN

Pesatnya kemajuan teknologi informasi dan komunikasi telah memberikan pengaruh besar pada berbagai aspek kehidupan, termasuk lingkungan perguruan tinggi. Sejalan dengan karakteristiknya sebagai *digital native*, mahasiswa saat ini sangat bergantung pada perangkat digital untuk memenuhi kebutuhan akademik, interaksi sosial, serta urusan personal mereka.. Walaupun memberikan kemudahan, ekspansi penggunaan teknologi digital juga memperbesar peluang terjadinya serangan siber. Ancaman seperti pencurian identitas, penyebaran *malware*, dan penyalahgunaan data menjadi isu serius yang menuntut kewaspadaan lebih tinggi di kalangan mahasiswa.

Berbagai penelitian menunjukkan bahwa tingkat kesadaran keamanan siber mahasiswa masih belum memadai. Alqahtani [1] menemukan bahwa meskipun mahasiswa memiliki pemahaman dasar tentang keamanan seperti penggunaan kata sandi, penggunaan *browser*, dan aktivitas di media sosial, praktik yang diterapkan seringkali masih jauh dari ideal. Hal serupa juga diungkapkan oleh Chasanah dan Candiwan [2] dalam studi mereka di Indonesia, bahwa mahasiswa cenderung belum memiliki perilaku aman dalam menghadapi ancaman seperti *phishing*, penggunaan konten ilegal, dan kebiasaan menggunakan password yang lemah.

Masalah semakin kompleks ketika menyinggung aspek respons dan pemulihan terhadap insiden digital. Banyak mahasiswa belum memiliki pengetahuan memadai mengenai langkah-langkah respons dan pemulihan sistem yang diperlukan ketika menjadi target serangan siber. Beberapa bahkan mengabaikan kejadian tersebut tanpa tindakan lanjutan, seperti tidak melaporkan insiden, tidak mengganti

e-ISSN: 2548-6861

password, atau tidak melakukan pemulihan data. Goliath, n.d. [3] menyebut fenomena ini sebagai *cybersecurity-resilience gap*, yaitu kesenjangan antara pengetahuan teoretis dengan perilaku nyata dalam menghadapi insiden digital.

Lebih lanjut, Sonhera et al. [4] dalam penelitiannya tentang penanganan insiden siber di sekolah-sekolah Afrika Selatan, menemukan bahwa ketiadaan prosedur penanganan insiden dan kurangnya panduan pelaporan menjadi faktor utama yang memperburuk dampak serangan siber. Jika hal ini terjadi di lingkungan pendidikan dasar, sangat mungkin bahwa situasi serupa juga terjadi di lingkungan perguruan tinggi, termasuk di Indonesia.

Mariam Jolo et al. [5] mengungkapkan bahwa faktor sosial juga mempengaruhi perilaku keamanan mahasiswa. Meskipun banyak dari mereka percaya diri terhadap kemampuan menjaga keamanan digital pribadi, Kenyataannya, masih banyak pula individu yang tetap melakukan tindakan berisiko, seperti membuka tautan dari sumber yang tidak jelas, menggunakan kata sandi yang lemah pada akun digital, dan tidak melakukan pencadangan data.

Untuk menjawab tantangan tersebut, kerangka kerja keamanan siber yang sistematis sangat dibutuhkan. Salah satu kerangka kerja yang telah banyak diadopsi secara internasional adalah *NIST Cybersecurity Framework (CSF)* yang dikembangkan oleh *National Institute of Standards and Technology (NIST)*, Amerika Serikat. *Framework* ini terdiri dari lima fungsi utama, yaitu: *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*. Fungsi *Respond* dan *Recover* memegang peranan penting dalam menangani dan memulihkan kondisi pasca-insiden siber.

## II. LANDASAN TEORI

### A. Perilaku Keamanan Siber

Perilaku keamanan siber merujuk pada tindakan nyata individu dalam melindungi data dan identitas digital dari berbagai ancaman. Perilaku ini dapat mencakup cara penggunaan kata sandi, respons terhadap email mencurigakan, hingga kebiasaan menggunakan perangkat atau jaringan. Menurut Mariam Jolo et al [5], terdapat beberapa faktor yang memengaruhi perilaku keamanan siber mahasiswa, antara lain:

1) Motivasi pribadi
   Mahasiswa yang memiliki pengalaman pribadi atau motivasi kuat dalam menjaga privasi cenderung lebih waspada terhadap ancaman digital.
2) Norma sosial
   Pengaruh dari lingkungan sekitar, termasuk teman sebaya dan budaya kampus, memiliki dampak besar terhadap praktik keamanan yang diterapkan.
3) Kebijakan kampus
   Adanya peraturan dan edukasi keamanan digital dari institusi dapat membentuk kebiasaan aman dalam aktivitas daring mahasiswa.

### B. Kesadaran Keamanan siber

Kesadaran keamanan siber merupakan pemahaman individu mengenai berbagai potensi ancaman digital serta upaya yang dapat dilakukan untuk melindungi diri dari risiko tersebut. Kesadaran ini meliputi tiga dimensi utama, yaitu pengetahuan, sikap, dan tindakan. Alqahtani [1] menyatakan bahwa semakin tinggi kesadaran seseorang terhadap risiko digital, semakin besar kemungkinan mereka akan melakukan tindakan perlindungan yang benar, seperti tidak membagikan informasi pribadi secara sembarangan.

### C. *NIST Cybersecurity Framework*

*NIST Cybersecurity Framework (CSF)* merupakan kerangka kerja yang dikembangkan oleh *National Institute of Standards and Technology (NIST)* untuk membantu organisasi dalam mengidentifikasi, mengelola, dan mengurangi risiko keamanan siber [6]. Kerangka kerja ini terdiri atas lima fungsi inti, yaitu *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*. Dalam penelitian ini, fokus pembahasan diarahkan pada dua fungsi utama, yaitu *Respond* dan *Recover*.

Fungsi *Respond* meliputi tindakan yang diambil untuk menanggapi insiden keamanan siber, termasuk mitigasi, pelaporan, dan komunikasi. Sedangkan fungsi *Recover* berkaitan dengan langkah-langkah pemulihan sistem, peningkatan berkelanjutan, dan pengembalian ke kondisi normal setelah terjadi gangguan.

*NIST CSF* telah menjadi standar acuan global yang fleksibel dan dapat diterapkan oleh berbagai jenis organisasi, termasuk lembaga pendidikan. Dengan menggunakan *framework* ini, penelitian dapat dilakukan dengan lebih terarah dan berdasarkan indikator yang jelas.

### D. Literasi Digital

Literasi digital merupakan kemampuan individu dalam memahami, mengevaluasi, serta memanfaatkan informasi digital secara bijak, kritis, dan aman. Menurut Rafi et al [7] mahasiswa yang memiliki pengalaman langsung dengan ancaman digital cenderung menunjukkan tingkat literasi yang lebih tinggi dalam menjaga privasi dan keamanan akun media

sosial. Literasi digital bukan hanya soal tahu teknologi, tetapi juga soal kesadaran etika, keamanan, dan kemampuan mengambil tindakan saat terjadi insiden.

E. Penelitian Terkait

Beberapa penelitian terdahulu yang relevan dengan kesadaran dan perilaku keamanan siber mahasiswa diuraikan berikut ini

Chasanah dan Candiwan [2] menganalisis tingkat kesadaran keamanan siber mahasiswa pada beberapa aspek keamanan digital menggunakan metode Analytic Hierarchy Process (AHP). Hasil penelitian menunjukkan bahwa tingkat kesadaran mahasiswa tergolong baik, meskipun masih terdapat aspek yang perlu ditingkatkan.

Sonhera et al. [4] mengkaji kesiapan institusi pendidikan dalam menangani insiden siber melalui pendekatan kualitatif. Penelitian tersebut menunjukkan perlunya prosedur penanganan insiden yang terstruktur.

Mariam Jolo et al. [5] meneliti faktor-faktor yang memengaruhi perilaku keamanan siber mahasiswa melalui survei daring. Hasilnya menunjukkan bahwa motivasi pribadi dan norma sosial memengaruhi perilaku keamanan mahasiswa.

Alqahtani [1] menganalisis pengaruh keamanan password, browser, dan media sosial terhadap kesadaran keamanan siber mahasiswa. Penelitian tersebut menunjukkan bahwa ketiga aspek tersebut berpengaruh signifikan terhadap tingkat kesadaran mahasiswa.

Rafi et al. [7] meneliti kesadaran privasi pengguna media sosial menggunakan pendekatan Technology Acceptance Model (TAM). Hasil penelitian menunjukkan bahwa pengalaman menghadapi ancaman siber dapat meningkatkan kewaspadaan pengguna.

Riyandhika dan Pratama [8] menganalisis faktor-faktor yang memengaruhi pengetahuan dan kesadaran keamanan siber mahasiswa menggunakan EFA dan SEM. Hasilnya menunjukkan bahwa faktor demografis berpengaruh terhadap tingkat kesadaran mahasiswa.

Hidayat et al. [9] mengidentifikasi perilaku preventif mahasiswa dalam menjaga keamanan digital melalui survei kuantitatif. Penelitian ini berfokus pada aspek pencegahan dan belum membahas penanganan maupun pemulihan insiden.

Ramadhanty [10] membandingkan kerangka NIST CSF dan ISO/IEC 27001 melalui studi literatur. Penelitian tersebut masih berfokus pada implementasi di tingkat organisasi.

Fahrizal et al. [11] meneliti kepatuhan mahasiswa terhadap praktik keamanan siber menggunakan pendekatan kuantitatif. Penelitian ini belum membahas tindakan pemulihan (Recover) setelah insiden siber.

Berdasarkan penelitian terdahulu, sebagian besar kajian berfokus pada kesadaran keamanan siber, perilaku pencegahan, dan kepatuhan terhadap kebijakan keamanan. Sementara itu, penelitian mengenai fungsi Respond dan Recover dalam kerangka NIST Cybersecurity Framework (CSF) pada konteks mahasiswa, khususnya di Politeknik Negeri Batam, masih terbatas sehingga menjadi dasar dilaksanakannya penelitian ini.

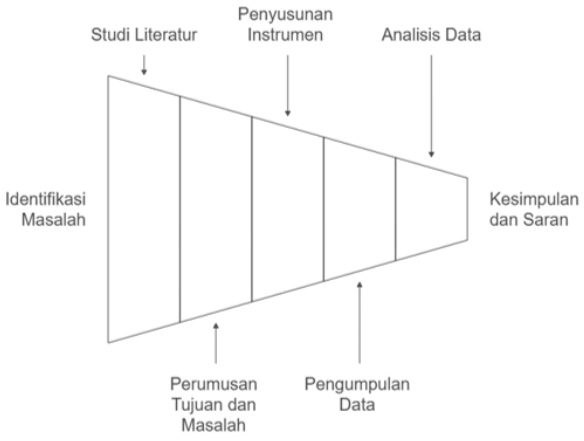
## III. METODE PENELITIAN

A. Pendekatan Penelitian

Penelitian ini menggunakan metode kuantitatif dengan pendekatan deskriptif. Pendekatan ini bertujuan untuk menggambarkan secara sistematis perilaku mahasiswa dalam aspek *Respond* dan *Recover* berdasarkan data yang diperoleh melalui kuesioner, tanpa menguji hubungan sebab-akibat (hipotesis) antarvariabel.

Data primer dikumpulkan melalui penyebaran kuesioner online kepada mahasiswa aktif Politeknik Negeri Batam. Data tersebut dianalisis menggunakan bantuan perangkat lunak SPSS untuk uji validitas konstruk melalui *Exploratory Factor Analysis (EFA)*, uji reliabilitas dengan *Cronbach's Alpha*, serta analisis statistik deskriptif.

Metodologi penelitian ini mengacu pada tahapan sistematis dalam metode kuantitatif yang dikemukakan oleh Sugiyono (2019), meliputi identifikasi masalah, studi literatur, perumusan tujuan dan masalah penelitian, penyusunan instrumen penelitian, pengumpulan data, analisis data, serta penarikan kesimpulan. Seluruh tahapan penelitian tersebut disajikan secara visual pada Gambar 1 dan dijelaskan secara rinci pada Tabel 1.




Gambar 1. Metode Penelitian

Berikut merupakan table yang berisi penjelasan dari gambar di atas.

e-ISSN: 2548-6861

Tabel I. Penjelasan Metode Penelitian

| Tahap | Deskripsi | Output |
|---|---|---|
| Identifikasi Masalah | Menentukan isu utama, yaitu rendahnya kesadaran dan respons mahasiswa terhadap ancaman digital. | Latar belakang dan rumusan masalah |
| Studi Literatur | Mencari dan menelaah jurnal yang relevan dengan topik penelitian untuk mengidentifikasi pendekatan, teori, dan hasil penelitian terdahulu. | Kajian Pustaka, landasan teori, dan kerangka pemikiran |
| Perumusan Tujuan dan Rumusan Masalah | Menyusun tujuan penelitian dan merumuskan pertanyaan yang ingin dijawab melalui penelitian. | Tujuan dan rumusan masalah yang terfokus |
| Penyusunan Instrumen | Menyusun kuisioner berdasarkan indikator-indikator dari pilar *Respond* dan *Recover* sesuai dengan *NIST framework*. | Draft kuisioner skala *Likert* |
| Pengumpulan Data | Menyebarkan Kuisioner kepada mahasiswa Politeknik Negeri Batam secara daring. | Data kuantitatif dari responden |
| Analisis Data | Mengelola hasil kuisioner menggunakan analisis statistik deskriptif. | Hasil analisis dan visualisasi data |
| Kesimpulan dan Saran | Menarik kesimpulan berdasarkan data dan memberikan rekomendasi yang relevan terhadap hasil temuan. | Kesimpulan akhir dan saran |

B. Ruang Lingkup penelitian

Penelitian ini dilakukan di lingkungan Politeknik Negeri Batam dengan melibatkan mahasiswa yang berasal dari berbagai program studi. Fokus utama dari penelitian ini adalah menganalisis pemahaman dan kesadaran mahasiswa dalam menghadapi ancaman digital, khususnya pada aspek respons dan pemulihan insiden siber berdasarkan dua pilar *NIST framework*

Ruang lingkup variabel yang dianalisis meliputi:

1) Variabel *Respond* mencakup beberapa indikator, yaitu *Incident Management, Incident Analysis, Reporting & Communication,* dan *Incident Mitigation.*
2) Variabel *Recover*, meliputi indikator *Incident Recovery Plan Execution* dan *Incident Recovery Communication*

C. Populasi dan Sampel

Populasi dalam penelitian ini adalah mahasiswa aktif Politeknik Negeri Batam dari berbagai jurusan dan program studi, dengan jumlah sekitar 11.329 mahasiswa. Karena jumlah populasi yang besar, penentuan sampel dalam penelitian ini menggunakan teknik *purposive sampling*, yaitu metode pemilihan sampel berdasarkan kriteria atau pertimbangan tertentu. Adapun kriteria sampel yang digunakan dalam penelitian ini adalah sebagai berikut:

1) Mahasiswa aktif
2) Bersedia menjadi responden secara sukarela
3) Mengisi kuesioner daring dengan lengkap

Jumlah minimum sampel ditentukan menggunakan rumus Slovin dengan tingkat kesalahan sebesar 10%, sehingga diperoleh jumlah sampel minimal sebanyak 100 responden. Sampel penelitian ini terdiri atas mahasiswa aktif yang bersedia berpartisipasi dengan mengisi kuesioner secara daring. Perhitungan jumlah minimum responden menggunakan rumus Slovin adalah sebagai berikut:

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

Dengan:

N = 11.329 (jumlah populasi)
$e$ = 0,10 (*margin of error* 10%)

$$n = \frac{11.329}{1 + 11.329(0{,}10)}$$

$$n = \frac{11.329}{1+11.329(0{,}10^2)} = \frac{11.329}{1+11.329(0{,}01)} = \frac{11.329}{1+113{,}29} = \frac{11.329}{114{,}29} \approx 99{,}1$$

Dengan demikian, jumlah responden minimum yang dibutuhkan dalam penelitian ini adalah 100 mahasiswa.

D. Instrumen Penelitian

Instrumen yang digunakan dalam penelitian ini adalah angket atau kuesioner tertutup berbasis skala Likert 4 poin. Setiap pernyataan disusun untuk mengukur aspek respons dan pemulihan terhadap insiden digital. Skala yang digunakan mencerminkan tingkat frekuensi atau kesepakatan responden terhadap pernyataan, yaitu:

1 = Tidak pernah
2 = Jarang
3 = Sering
4 = Selalu

Kuesioner dibagi menjadi dua bagian utama:

1) Bagian pertama berisi pertanyaan demografis yang bertujan untuk menetahui karakteristik responden, meliputi: usia, jenis kelamin, jurusan, semester saat ini
2) Bagian kedua terdiri atas pertanyaan-pertanyaan yang mengukur pengetahuan dan kesadaran keamanan siber berdasarkan pilar *Response* dan *Recover*.

Setiap variabel *(Respond* dan *Recover)* dikonstruksi menjadi beberapa indikator yang disusun mengacu pada *NIST Cybersecurity Framework 2.0*, dengan sejumlah rujukan indikator diadaptasi dari jurnal Rizky Riyandhika et al. [8]. Total butir pernyataan awal berjumlah 20 butir, terdiri atas 13 butir untuk variabel *Respond* dan 7 butir untuk variabel *Recover*.

E. Validasi dan Uji Coba Instrumen

Sebelum diterapkan pada penelitian utama, instrumen kuesioner terlebih dahulu dilakukan proses validasi melalui expert judgement. Proses ini dilakukan dengan mengonsultasikan kuesioner kepada dosen pembimbing yang sekaligus melakukan pengujian langsung dengan cara mengisi kuesioner untuk mengevaluasi kejelasan, kesesuaian, dan kelengkapan butir pertanyaan yang disusun.

Berdasarkan hasil evaluasi tersebut, dilakukan perbaikan pada beberapa bagian kuesioner hingga dinyatakan layak digunakan. Setelah memperoleh persetujuan dari dosen pembimbing, kuesioner kemudian langsung disebarkan kepada responden penelitian.

1) Validitas isi dievaluasi melalui expert judgement oleh dosen pembimbing. Uji validitas konstruk tetap dilakukan menggunakan Exploratory Factor Analysis (EFA) dengan bantuan software SPSS. Butir pernyataan dengan nilai loading factor > 0,5 dianggap valid.
2) Reliabilitas instrumen diuji menggunakan metode Cronbach's Alpha, dengan nilai > 0,6 sehingga instrumen dinyatakan reliabel.

Dengan proses validasi yang telah dilakukan, kuesioner dianggap layak sebagai instrumen utama dalam pengumpulan data pada penelitian ini.

F. Teknik Pengumpulan Data

Proses pengumpulan data dilakukan secara daring dengan mendistribusikan tautan kuesioner kepada mahasiswa melalui berbagai platform komunikasi, seperti WhatsApp dan Instagram. Sebelum mengisi kuesioner, responden terlebih dahulu memperoleh penjelasan mengenai tujuan penelitian, jaminan kerahasiaan identitas, serta ketentuan untuk mengisi seluruh butir pertanyaan guna memastikan kelengkapan data yang akan dianalisis.

Penyebaran kuesioner dilaksanakan pada tanggal 25 Mei 2026 hingga 9 Juli 2026, sedangkan tahap pengolahan data dilakukan pada tanggal 9–12 Juli 2026. Penggunaan kuesioner berbasis daring dipilih karena memberikan kemudahan akses bagi responden melalui perangkat pribadi, sehingga proses pengumpulan data dapat dilakukan secara lebih efisien dan menjangkau partisipan dalam jumlah yang lebih besar.

G. Teknik Analisis Data

Analisis data pada penelitian ini dilakukan secara bertahap dan sistematis guna memastikan bahwa hasil penelitian yang diperoleh memiliki tingkat validitas, reliabilitas, serta dapat dipertanggungjawabkan secara ilmiah. Tahapan analisis data dibagi menjadi tiga bagian utama, yaitu: analisis faktor eksploratori (EFA) untuk uji validitas konstruk, uji reliabilitas dengan *Cronbach's Alpha*, dan analisis statistik deskriptif. Tahapan-tahapan ini mengikuti kerangka analisis kuantitatif deskriptif sebagaimana dijelaskan oleh Sugiyono (2019). Berikut adalah penjelasan detail alur dan mekanismenya:

1) Pengolahan Data Awal

e-ISSN: 2548-6861

- Data dari kuesioner daring diekspor ke format spreadsheet (Excel/CSV) dan kemudian diimpor ke SPSS.
- Data dibersihkan dari respon tidak lengkap, duplikat, atau inkonsistensi.
- Setiap butir pertanyaan dikodekan dalam bentuk numerik (skala Likert 1-4)

2) Analisis Deskriptif
   - Digunakan untuk memberikan gambaran umum mengenai karakteristik responden, meliputi usia, jenis kelamin, program studi, dan semester yang sedang ditempuh.
   - Dihitung nilai rata-rata, persentase, dan standar deviasi untuk setiap butir pertanyaan.
   - Hasil ini digunakan untuk mengetahui kecenderungan jawaban responden secara umum terhadap masing-masing indikator.
3) Uji Validitas dan Realibilitas
   - Uji validitas konstruk pada penelitian ini dilakukan menggunakan *Exploratory Factor Analysis (EFA)*. Analisis faktor dapat diterapkan apabila nilai Kaiser-Meyer-Olkin (KMO) ≥ 0,6, yang menunjukkan bahwa data memiliki kelayakan untuk dilakukan analisis faktor. Selain itu, *Bartlett's Test of Sphericity* harus menghasilkan nilai signifikansi ($p < 0,05$). Suatu faktor dinyatakan valid apabila memiliki nilai *loading factor* lebih dari 0,5. Dalam memperjelas struktur faktor yang terbentuk, penelitian ini menggunakan metode rotasi *Varimax*.
   - Uji reliabilitas dilakukan dengan menghitung nilai *Cronbach's Alpha* pada setiap konstruk penelitian. Suatu konstruk dapat dinyatakan reliabel apabila memperoleh nilai *Cronbach's Alpha* lebih besar dari 0,6.
4) Interpretasi dan Penarikan Kesimpulan
   - Hasil uji validitas (EFA), uji reliabilitas *(Cronbach's Alpha)*, dan analisis deskriptif digunakan untuk menggambarkan tingkat perilaku mahasiswa pada setiap indikator *Respond* dan *Recover*.
   - Hasil akhir dianalisis untuk menjawab rumusan masalah penelitian.
   - Kesimpulan digunakan sebagai dasar penyusunan saran bagi mahasiswa maupun institusi pendidikan.

Dengan alur analisis ini, penelitian memberikan gambaran deskriptif yang valid dan reliabel mengenai perilaku mahasiswa dalam merespons dan memulihkan diri dari insiden keamanan siber pada pilar *Respond* dan *Recover*.

## IV. HASIL DAN PEMBAHASAN

A. Karakteristik Responden

Penelitian melibatkan 101 responden mahasiswa aktif Politeknik Negeri Batam dari berbagai jurusan.

Tabel II. Karakteristik Responden (N=101)

| Kategori | Kelompok | n (%) |
|---|---|---|
| Jenis Kelamin | Laki-laki | 30 (29,7%) |
| | Perempuan | 71 (70,3%) |
| Usia | 18-19 tahun | 7 (6,9%) |
| | 20-21 tahun | 51 (50,5%) |
| | 22-23 tahun | 39 (38,6%) |
| | 24-25 tahun | 4 (4,0%) |
| Semester | 2 | 6 (5,9%) |
| | 4 | 17 (16,8%) |
| | 6 | 46 (45,5%) |
| | 8 | 32 (31,7%) |
| Jurusan | Teknik Informatika | 42 (41,6%) |
| | Manajemen Bisnis | 36 (35,6%) |
| | Teknik Elektro | 12 (11,9%) |
| | Teknik Mesin | 11 (10,9%) |

Mayoritas responden berjenis kelamin perempuan (70,3%), berusia 20-21 tahun (50,5%), semester 6 (45,5%), dan berasal dari Jurusan Teknik Informatika (41,6%), dengan Program Studi Rekayasa Keamanan Siber sebagai penyumbang terbesar (19 responden).

Dominasi responden dari Jurusan Teknik Informatika menjadi salah satu karakteristik yang perlu diperhatikan dalam memahami hasil penelitian ini. Mahasiswa pada jurusan tersebut, termasuk mahasiswa Program Studi Rekayasa Keamanan Siber, umumnya memperoleh paparan materi keamanan siber yang lebih intensif dibandingkan mahasiswa dari jurusan lain. Kondisi tersebut menyebabkan temuan penelitian ini lebih banyak merepresentasikan perilaku *Respond* dan *Recover* pada mahasiswa dengan tingkat literasi digital yang relatif tinggi. Dengan demikian, hasil penelitian ini menggambarkan kondisi responden yang terlibat dan belum sepenuhnya merepresentasikan keragaman karakteristik seluruh mahasiswa Politeknik Negeri Batam.

.B. Hasil Uji Validitas dan Reliabilitas

Uji validitas konstruk dilakukan dengan *Exploratory Factor Analysis (EFA)* menggunakan ekstraksi *Principal Component Analysis* dan rotasi *Varimax* terhadap 20 butir awal instrumen (RS1-RS13 dan RC1-RC7) yang disebarkan kepada 101 responden mahasiswa aktif Politeknik Negeri Batam.

Tabel III. KMO and Bartlett's Test

| Uji | Nilai |
|---|---|
| Kaiser-Meyer-Olkin (KMO) | 0,896 |
| Bartlett's Test - Chi-Square | 1260,034 |
| Bartlett's Test - df | 190 |
| Bartlett's Test - Sig. | 0,000 |

Nilai KMO sebesar 0,896 (kategori meritorious) dan *Bartlett's Test* signifikan (p = 0,000) menunjukkan data layak dianalisis faktor.

Tabel IV. Total Variance Explained (Rotation)

| Komp. | Total | % Var. | Kum. % |
|---|---|---|---|
| 1 | 3,660 | 18,298 | 18,298 |
| 2 | 3,362 | 16,812 | 35,110 |
| 3 | 3,245 | 16,225 | 51,335 |
| 4 | 3,174 | 15,871 | 67,206 |

Empat komponen terbentuk dengan total varians kumulatif 67,206% (>60%). Butir RS1, RS13, RC1, dan RC6 tidak menunjukkan *loading factor* yang jelas (<0,50) pada *Rotated Component Matrix* sehingga dinyatakan gugur. Butir valid yang digunakan pada analisis selanjutnya berjumlah 11 butir *Respond* (RS2-RS12) dan 5 butir *Recover* (RC2, RC3, RC4, RC5, RC7).

Tabel V. Hasil Uji Reliabilitas

| Variabel | Butir | Alpha | Kategori |
|---|---|---|---|
| Respond | 11 | 0,880 | Sangat Baik |
| Recover | 5 | 0,847 | Sangat Baik |

Kedua variabel memperoleh nilai *Cronbach's Alpha* di atas 0,70, sehingga instrumen penelitian dinyatakan memiliki tingkat reliabilitas yang baik dan konsisten.

C. Hasil Analisis Deskriptif

Kategorisasi tingkat perilaku menggunakan interval kelas skala Likert 1-4: 1,00-1,75 (Tidak Pernah), 1,76-2,50 (Jarang), 2,51-3,25 (Sering), 3,26-4,00 (Selalu).

Tabel VI. Statistik Deskriptif Butir Penelitian

| Var. | Butir | Mean | SD | Kategori |
|---|---|---|---|---|
| Respond | RS2 | 2,82 | 1,014 | Sering |
| Respond | RS3 | 2,97 | 0,964 | Sering |
| Respond | RS4 | 3,33 | 0,850 | Selalu |
| Respond | RS5 | 3,28 | 0,814 | Selalu |
| Respond | RS6 | 2,71 | 1,033 | Sering |
| Respond | RS7 | 3,12 | 0,972 | Sering |
| Respond | RS8 | 2,98 | 0,990 | Sering |
| Respond | RS9 | 3,36 | 0,795 | Selalu |
| Respond | RS10 | 3,30 | 0,878 | Selalu |
| Respond | RS11 | 3,47 | 0,769 | Selalu |
| Respond | RS12 | 2,85 | 0,974 | Sering |
| Recover | RC2 | 3,04 | 0,969 | Sering |
| Recover | RC3 | 3,41 | 0,764 | Selalu |
| Recover | RC4 | 3,03 | 0,984 | Sering |
| Recover | RC5 | 3,34 | 0,816 | Selalu |
| Recover | RC7 | 3,37 | 0,857 | Selalu |

Tabel VII. Rekapitulasi Rata-rata per Indikator

| Var. | Indikator | Rata2 | Kategori |
|---|---|---|---|
| Respond | Incident Management | 2,895 | Sering |
| Respond | Incident Analysis | 3,107 | Sering |
| Respond | Reporting & Communication | 3,153 | Sering |
| Respond | Incident Mitigation | 3,207 | Sering |
| Recover | Incident Recovery Plan Execution | 3,225 | Sering |
| Recover | Incident Recovery Communication | 3,247 | Sering |

Rata-rata keseluruhan variabel Respond sebesar 3,107 dan Recover sebesar 3,236, keduanya kategori Sering. Butir dengan mean tertinggi adalah RS11 (3,47, *Incident Mitigation*) dan terendah RS6 (2,71, *Incident Analysis*). Pada *Recover*, RC3 (3,41) tertinggi dan RC4 (3,03) terendah.

D. Pembahasan

Instrumen penelitian ini valid secara konstruk (KMO 0,896; *Bartlett's Test* signifikan; varians terjelaskan 67,206%) dan reliabel (*Alpha Respond* 0,880; *Recover* 0,847), sehingga temuan deskriptif berikut dapat dipertanggungjawabkan secara ilmiah.

Secara umum, mahasiswa Politeknik Negeri Batam menunjukkan frekuensi perilaku Sering hingga Selalu dalam merespons dan memulihkan diri dari insiden siber. Temuan ini berbeda dari kondisi yang digambarkan Alqahtani [1] maupun Chasanah dan Candiwan [2], yang menemukan praktik keamanan mahasiswa masih jauh dari ideal; perbedaan ini kemungkinan disebabkan oleh fokus penelitian yang berbeda, yaitu perilaku pasca-insiden (*Respond* dan *Recover*) dibandingkan perilaku pencegahan sehari-hari yang menjadi fokus penelitian sebelumnya.

Indikator *Incident Management* menunjukkan rata-rata terendah pada pilar *Respond*, sejalan dengan temuan Sonhera

e-ISSN: 2548-6861

[4] bahwa ketiadaan prosedur penanganan insiden yang jelas menjadi titik lemah utama dalam respons terhadap insiden siber. Hal ini mengindikasikan bahwa meskipun mahasiswa cukup responsif dalam mitigasi dan pelaporan, aspek pengelolaan/koordinasi awal penanganan insiden masih perlu diperkuat.

Perlu dicatat bahwa data bersifat *self-reported*, sehingga tingkat frekuensi yang tinggi tidak serta-merta mencerminkan efektivitas tindakan yang diambil. Kesenjangan antara frekuensi tindakan dan kualitas/ketepatan tindakan tersebut sejalan dengan konsep *cybersecurity-resilience gap* yang diajukan oleh Goliath [3] Sebagai penelitian deskriptif tanpa pengujian hipotesis, temuan ini menggambarkan pola perilaku pada saat penelitian dilakukan dan tidak dimaksudkan untuk menyimpulkan hubungan sebab-akibat antar indikator maupun antar pilar.

## V. KESIMPULAN

Instrumen penelitian pada pilar *Respond* dan *Recover* dinyatakan valid (EFA: KMO 0,896; *Bartlett's Test* signifikan; varians terjelaskan 67,206% melalui 4 komponen) dan reliabel (*Cronbach's Alpha Respond* 0,880; *Recover* 0,847). Butir valid berjumlah 11 untuk *Respond* (RS2-RS12) dan 5 untuk *Recover* (RC2, RC3, RC4, RC5, RC7).

Hasil analisis deskriptif menunjukkan bahwa perilaku mahasiswa pada seluruh butir kedua variabel berada pada kategori Sering hingga Selalu, dengan rata-rata keseluruhan Respond 3,107 dan *Recover* 3,236 (kategori Sering). Indikator *Incident Mitigation* menunjukkan tingkat tertinggi pada pilar *Respond*, sedangkan *Incident Management* menunjukkan tingkat terendah, mengindikasikan area yang perlu diperkuat dalam edukasi keamanan siber di lingkungan kampus.

Penelitian selanjutnya disarankan melakukan *Confirmatory Factor Analysis (CFA)* atau *Structural Equation Modeling (SEM)* apabila hendak menguji kesesuaian model faktor teoritis secara lebih ketat atau menguji hubungan pengaruh antar-pilar *Respond* dan *Recover* secara inferensial.

## DAFTAR PUSTAKA


[1] M. A. Alqahtani, “Factors Affecting Cybersecurity Awareness among University Students,” *Applied Sciences (Switzerland)*, vol. 12, no. 5, Mar. 2022, doi: 10.3390/app12052589.

[2] B. R. Chasanah and C. Candiwan, “Analysis of College Students’ Cybersecurity Awareness In Indonesia,” *SISFORMA*, vol. 7, no. 2, pp. 49–57, Nov. 2020, doi: 10.24167/sisforma.v7i2.2706.

[3] S. Goliath, “Exploring the Cybersecurity-Resilience Gap: An Analysis of Student Attitudes and Behaviors in Higher Education.”

[4] N. Sonhera, E. Kritzinger, and M. Loock, “Cyber Incident Handling and the Perceptions of Learners on Cyber Incidents in South African Schools,” *Advances in Science, Technology and Engineering Systems Journal*, vol. 6, no. 5, pp. 23–31, Sep. 2021, doi: 10.25046/aj060504.

[5] S. M. Mariam Jolo, S. A. Salain, and S. S. Hanna Abah, “International Journal of Multidisciplinary Research and Publications A Socio-Technical Perspective,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, vol. 5, no. 10, pp. 117–125, 2023.

[6] “The NIST Cybersecurity Framework (CSF) 2.0,” Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[7] M. Rafi, S. Pane, E. Wilson, Q. Awfa, and A. Karim, “Pemahaman Keamanan Dan Perlindungan Privasi Menurut Pandangan Generasi Milenial,” *Portal Riset dan Inovasi Sistem Perangkat Lunak*, vol. 3, no. 1, pp. 39–44, Jan. 2025, doi: 10.59696/prinsip.v3i1.81.

[8] R. Rizky Riyandhika, A. Raf, and ie Pratama, “Analisis Kesadaran Cybersecurity pada Kalangan Mahasiswa di Indonesia.”

[9] A. Hidayat, M. J. Awaliyah, A. Abdillah, F. Rachman, A. M. A. Am, and J. Teknik, “Fundamental and Applied Management Journal Analisis Perilaku Mahasiswa dari Ancaman Keamanan Komputer,” *Juni*, vol. 1, no. 1, 2023.

[10] N. Ramadhanty, “Implementasi Kerangka Keamanan NIST Dan ISO/IEC 27001 Dalam Menghadapi Ancaman Risiko Siber,” *Journal of Indonesian Management*, vol. 4, no. 4, Nov. 2024, doi: 10.53697/jim.v4i4.1973.

[11] M. F. A. Yakin, I. A. F. Fahrizal, H. Dewantara, A. N. Q. Azisah, Alisyahbana, and S. Diarra, “Pengaruh Hipersekuritisasi dan Praktik Keamanan Siber Harian Terhadap Kepatuhan Mahasiswa dalam Menghadapi Ancaman Digital,” Jan. 2025.