MARKAS BESAR ANGKATAN LAUT
AKADEMI

Perbaikan :
Ringan / Sedang / Berat
Ketua Tim Penguji

ANALISIS MANAJEMEN RISIKO BAHAYA *CYBER CRIME IDENTITY THEFT* TERHADAP PERSONEL AKADEMI TNI ANGKATAN LAUT

SKRIPSI

OLEH:

GUSTI SAPTO GUMELAR

SERMATAR (P) NO. AK. 2021.466

PROGRAM STUDI MANAJEMEN PERTAHANAN MATRA LAUT

AKADEMI TNI ANGKATAN LAUT

SURABAYA

2025

ANALISIS MANAJEMEN RISIKO BAHAYA *CYBER CRIME IDENTITY THEFT* TERHADAP PERSONEL AKADEMI TNI ANGKATAN LAUT

SKRIPSI

DIAJUKAN GUNA MEMENUHI SALAH SATU PERSYARATAN KELULUSAN SARJANA TERAPAN PERTAHANAN PROGRAM STUDI MANAJEMEN PERTAHANAN MATRA LAUT

OLEH:
GUSTI SAPTO GUMELAR
SERMATAR (P) NO. AK. 2021.466

PROGRAM STUDI MANAJEMEN PERTAHANAN MATRA LAUT
AKADEMI TNI ANGKATAN LAUT
SURABAYA
2025

HALAMAN ORISINALITAS SKRIPSI

Nama	: Gusti Sapto Gumelar
Pangkat/Korps/No.AK	: Sermatar (P) No. AK. 2021.466
Program Studi	: Manajemen Pertahanan Matra Laut
Judul	: Analisis Manajemen Risiko Bahaya *Cyber Crime Identity Theft* Terhadap Personel Akademi TNI Angkatan Laut

Saya menyatakan dengan sebenar-benarnya sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu Perguruan Tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah skripsi ini dapat dibuktikan unsur-unsur PLAGIASI, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (Sarjana Terapan Pertahanan) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Surabaya, 27 Mei 2025

Yang Menyatakan,

Gusti Sapto Gumelar

Sermatar (P) No. AK. 2021.466

HALAMAN PERSETUJUAN

Skripsi ini diajukan oleh	:	
Nama	:	Gusti Sapto Gumelar
Pangkat/Korps/No. AK	:	Sermatar (P) No. AK. 2021.466
Program Studi	:	Manajemen Pertahanan Matra Laut
Judul Skripsi	:	Analisis Manajemen Risiko Bahaya *Cyber Crime Identity Theft* Terhadap Personel Akademi TNI Angkatan Laut

Menyetujui/Mengetahui untuk diuji pada ujian skripsi oleh: Pembimbing I	Menyetujui/Mengetahui untuk diuji pada ujian skripsi oleh: Pembimbing II
Eko Hadi Suwarno,CBEI.,M.Tr.Opsla. Mayor Laut (P) NRP 19179/P	Nur Cahyo Utomo, S.H.,M.Tr.Opsla. Letkol Laut (E) NRP 18251/P

Mengetahui,
Kepala Program Studi

Pungki Kurniawan, M. Tr. Opsla.
Letkol Laut (P) NRP 16539/P

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh	:	
Nama	:	Gusti Sapto Gumelar
Pangkat/Korps/No. AK	:	Sermatar (P) No. AK. 2021.466
Program Studi	:	Manajemen Pertahanan Matra Laut
Judul Skripsi	:	Analisis Manajemen Risiko Bahaya *Cyber Crime Identity Theft* Terhadap Personel Akademi TNI Angkatan Laut

Telah berhasil dipertahankan di hadapan Dewan Penguji Ujian Skripsi pada Program Studi Manajemen Pertahanan Matra Laut, Akademi TNI Angkatan Laut.

DISAHKAN OLEH:

Dosen Pembimbing I	:	Eko Hadi Suwarno, CBEI.,M.Tr.Opsla. Mayor Laut (P) NRP 19179/P	( )
Dosen Pembimbing II	:	Nur Cahyo Utomo, S.H.,M.Tr.Opsla. Letkol Laut (E) NRP 18251/P	( )
Ketua Penguji	:	Pius Herdasa Krisna Murti, S.T., M.T., CBEI., CACA., CRMP., CHRMP. Letkol Laut (P) NRP 15395/P	( )
Penguji I	:	Suhendra, S.Ag., M.A.P. Letkol Laut (KH) NRP 13023/P	( )
Penguji II	:	Pradipta Dewantara, S.S.T.Han Mayor Laut (P) NRP 19915/P	( )
Sekretaris	:	Abdul Ra'uf, S.Tr.Han Letda Laut (P) NRP 24508/P	( )
Ditetapkan di	:	Surabaya	
Tanggal	:	27 Mei 2025	

Mengetahui,
Kepala Program Studi

Pungki Kurniawan, M.Tr.Opsla
Letnan Kolonel Laut (P) NRP 16539/P

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Akademi TNI Angkatan Laut, saya yang bertanda tangan dibawah ini:

Nama	: Gusti Sapto Gumelar
Pangkat/Korps/No. AK	: Sermatar (P) No. AK. 2021.466
Program Studi	: Manajemen Pertahanan Matra Laut
Departemen	: Pelaut
Jenis karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Akademi Angkatan Laut **Hak Bebas Royalti Non esklusif *(Non-exclusive Royalty Free Right)*** atas karya ilmiah saya yang berjudul:

"**ANALISIS MANAJEMEN RISIKO BAHAYA *CYBER CRIME IDENTITY THEFT* TERHADAP PERSONEL AKADEMI TNI ANGKATAN LAUT"**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non eksklusif ini Akademi Angkatan Laut berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data *(database)*, merawat dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
Demikian pernyataan ini saya buat dengan sebenarnya.

Surabaya, 27 Mei 2025
Yang menyatakan,

Gusti Sapto Gumelar
Sermatar (P) No. AK. 2021.466

ABSTRAK

Penelitian ini bertujuan untuk menganalisis manajemen risiko bahaya *cyber crime identity theft* terhadap personel Akademi TNI Angkatan Laut (AAL). Kemajuan teknologi informasi membawa dampak positif, namun juga meningkatkan risiko kejahatan siber, termasuk pencurian identitas. Penelitian ini menggunakan metode HIRADC (Hazard Identification Risk Assessment and Determining Control) untuk mengidentifikasi dan menganalisis risiko, serta merumuskan tindak mitigasi yang tepat. Dalam penelitian ini, data dikumpulkan melalui wawancara dengan narasumber yang berkompeten di bidang keamanan siber di lingkungan AAL. Hasil penelitian menunjukkan bahwa risiko *cyber crime identity theft* tergolong tinggi, dengan variabel risiko utama seperti *malware, phishing, skimming, cracking,* dan *bullying*. Penelitian ini menemukan bahwa kesadaran personel AAL terhadap risiko ini masih rendah, sehingga diperlukan langkah-langkah mitigasi yang komprehensif. Rekomendasi yang dihasilkan meliputi peningkatan infrastruktur keamanan siber, sosialisasi tentang bahaya *cyber crime*, serta penguatan program pelatihan bagi personel. Dengan penerapan rekomendasi ini, diharapkan personel AAL dapat lebih siap menghadapi ancaman *cyber crime*, sehingga integritas dan keamanan data pribadi mereka dapat terjaga. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan keamanan siber di lingkungan TNI Angkatan Laut dan instansi terkait lainnya.

KATA PENGANTAR

Segala puji syukur atas limpahan rahmat dan hidayah dari Tuhan Yang Maha Esa, yang telah memberikan kekuatan lahir dan batin kepada penulis, sehingga dapat menyelesaikan skripsi ini dengan judul “ANALISIS MANAJEMEN RISIKO BAHAYA *CYBER CRIME IDENTITY THEFT* TERHADAP PERSONEL AKADEMI TNI ANGKATAN LAUT ”. Sebagai salah satu persyaratan untuk menyelesaikan pendidikan bagi Taruna Akademi TNI Angkatan Laut.

Berkat perhatian, bimbingan, dan dukungan dari pembimbing, perwira pembimbing, serta berbagai pihak yang tidak bisa disebutkan semuanya satu persatu, skripsi ini telah dapat diselesaikan tepat pada waktunya. Oleh karenanya penulis mengucapkan terima kasih dan penghargaan yang setinggi-tingginya kepada yang Terhormat:

1. Gubernur Akademi TNI Angkatan Laut, Laksamana Muda TNI Dato Rusman S.N., S.E., M.Si., M.Tr.Opsla.
2. Kepala Program Studi Manajemen Pertahanan Matra Laut Letnan Kolonel Laut (P) Pungki Kurniawan, M.Tr.Opsla.
3. Dosen Pembimbing Skripsi Mayor Laut (P) Eko Hadi Suwarno, CBEI., M.Tr.Opsla. dan Letkol Laut (E) Nur Cahyo Utomo, S.H.,M.Tr.Opsla.

Penulis menyadari bahwa skripsi ini masih belum sempurna dan memerlukan perbaikan untuk penyempurnaannya. Oleh karena itu, penulis menerima dengan tulus ikhlas, koreksi dan saran yang konstruktif dari pembaca dan semua pihak agar skripsi ini dapat digunakan sebagai bahan acuan tambahan didalam penyelesaian permasalahan di lingkungan Akademi TNI Angkatan Laut.

Akhirnya, semoga Tuhan Yang Maha Esa senantiasa memberikan rahmat dan petunjuk-Nya kepada kita semua dalam melanjutkan pengabdian kepada bangsa dan negara.

Surabaya, 27 Mei 2025

Yang menyatakan,

Gusti Sapto Gumelar

Sermatar (P) No. AK. 2021.466

DAFTAR ISI

BAB III METODE PENELITIAN

BAB IV PEMBAHASAN

BAB V PENUTUP

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR TABEL

HALAMAN

DAFTAR GAMBAR

HALAMAN

DAFTAR LAMPIRAN

HALAMAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajauan teknologi telah memberikan sumber (*resources*) informasi dan komunikasi yang amat luas dari apa yang telah dimiliki manusia. Meskipun peranan informasi dalam beberapa dekade kurang mendapat perhatian, namun sesungguhnya kebutuhan akan informasi dan komunikasi itu merupakan hal yang tidak kalah pentingnya dari kebutuhan sandang dan pangan manusia. Dunia telah beralih dari era industrialisasi ke era informasi yang kemudian melahirkan masyarakat informasi (*information society*) (Ahmad, 2012). Kemajuan teknologi komunikasi dan informasi tentunya erat kaitannya dengan internet. Penggunaan internet di Indonesia terus meningkat dari tahun ke tahun seiring dengan semakin luasnya akses internet dan adopsi teknologi digital di berbagai sektor. Berdasarkan data yang dirilis oleh Asosiasi Penyelenggara Jasa Internet Indonesia tahun 2022, jumlah pengguna internet di Indonesia mencapai sekitar 210 juta orang atau sekitar 78,4% dari total populasi Indonesia yang mencapai 267,7 juta jiwa (Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2022). Faktanya, teknologi digital yang berkembang pesat memiliki dampak negatif yang berisiko terhadap penyebaran informasi palsu dan ketergantungan pada teknologi. Perkembangan teknologi digital juga telah meningkatkan ancaman *cyber crime* secara signifikan, termasuk serangan *cracking, skimming, malware, hacking*, dan pencurian data pribadi. Serangan *cyber crime* juga berdampak pada pencurian identitas, kehilangan pekerjaan, dan gangguan terhadap infrastruktur kritis (Hapsari & Pambayun, 2023). Masyarakat khususnya personel AAL pada umumnya kurang sadar akan risiko *cyber crime* dan tidak memahami cara melindungi diri mereka sendiri secara efektif. Hukum dan regulasi seputar *cyber crime* juga terus berubah-ubah dalam ketidakpastian. Sementara itu pelaku cyber *crime* terus mengembangkan teknik dan strategi baru.

Dalam era digital yang semakin maju, ancaman kejahatan siber (*cyber crime)* menjadi semakin nyata dan beragam. Salah satu bentuk kejahatan siber yang sangat meresahkan adalah pencurian identitas (*identity theft*). Kejahatan ini melibatkan pengambilan informasi pribadi seseorang secara ilegal dengan tujuan untuk melakukan penipuan atau tindakan kriminal lainnya. Informasi pribadi yang

dicuri dapat mencakup nomor identifikasi pribadi, kata sandi, data keuangan, dan informasi sensitif lainnya yang bisa digunakan untuk merugikan korban. Personel AAL sebagai bagian dari instansi militer yang berperan penting dalam pertahanan negara, merupakan target potensial bagi pelaku kejahatan siber. Data pribadi mereka memiliki nilai tinggi dan dapat dimanfaatkan untuk berbagai tujuan, mulai dari penipuan keuangan hingga *spionase*. Selain itu, pencurian identitas dapat mengancam keamanan nasional jika informasi yang dicuri digunakan untuk mengakses data militer yang lebih sensitif. Mengingat AAL adalah suatu instansi militer yang menghasilkan para perwira TNI Angkatan Laut yang akan menjadi pemimpin di masa depan, sehingga perlu dilaksanakan upaya pencegahan kejahatan *cyber crime* agar tidak berpengaruh pada calon pemimpin masa depan.

Upaya ini mencakup berbagai aspek, mulai dari peningkatan kesadaran dan pendidikan personel tentang pentingnya keamanan data pribadi, hingga implementasi teknologi keamanan yang canggih untuk melindungi data sensitif. Dengan demikian, AAL dapat memastikan bahwa personelnya terlindungi dari ancaman *cyber crime*, sekaligus menjaga integritas dan keamanan informasi yang penting bagi keamanan nasional. Melalui upaya ini, diharapkan bahwa Akademi TNI Angkatan Laut dapat mengurangi risiko pencurian identitas dan dampak negatifnya, sekaligus memperkuat sistem keamanan siber yang ada. Dengan demikian, personel AAL dapat menjalankan tugas mereka dengan lebih aman dan fokus, tanpa khawatir akan ancaman *cyber crime* yang dapat mengganggu integritas dan keamanan mereka.

1.2 Permasalahan

a. Identifikasi Masalah.

Dari latar belakang diatas, maka diperoleh identifikasi masalah sebagai berikut:

1) Belum adanya identifikasi risiko bahaya *cyber crime identity theft* di Akademi TNI Angkatan Laut

2) Belum adanya analisis risiko bahaya *cyber crime identity theft* pada Personel Akademi TNI Angkatan Laut.

b. Rumusan Masalah.

Rumusan masalah dalam penulisan ini adalah:

1) Bagaimana identifikasi risiko bahaya *cyber crime identity theft*

di Akademi TNI Angkatan Laut?

2) Bagaimana peringkat risiko bahaya *cyber crime identity theft* terhadap Personel Akademi TNI Angkatan Laut?

1.3 Tujuan dan Manfaat

a. Tujuan

Penulisan hasil penelitian ini bertujuan untuk memberikan sumbangan pemikiran dan sebagai bahan masukan terkait hal-hal yang berdasarkan rumusan masalah sebagai berikut:

1) Mengidentifikasi risiko bahaya *cyber crime identity theft* di Akademi TNI Angkatan Laut.

2) Menganalisis peringkat risiko bahaya *cyber crime identity theft* terhadap Personel Akademi TNI Angkatan Laut.

3) Membuat tindak mitigasi berupa *cyber security* guna mengurangi risiko bahaya *cyber crime identity theft*.

b. Manfaat

1) Secara Teoritis

Hasil penelitian ini diharapkan bermanfaat menjadi sumbangan pemikiran dan kasanah kepustakaan dalam memberikan gambaran terkait analisis risiko bahaya *cyber crime identity theft* pada Personel Akademi TNI Angakatan Laut menggunakan metode Hiradc. Dengan analisis tersebut, diharapkan dapat menghasilkan gambaran risiko bahaya *cyber crime identity theft* yang memiliki tingkat risiko tinggi di AAL dan memberikan tindak mitigasi yang efektif berupa *cyber security* yang dapat diterapkan guna mengurangi risiko pada AAL.

2) Secara Praktis.

Hasil penelitian ini diharapkan dapat memberi manfaat praktis, yakni memberikan masukan bagi seluruh pemangku kebijakan terkait perkembangan ancaman *cyber crime identity theft* serta bahan pertimbangan pentingnya berupa penerapan *cyber security* pada personel AAL.

1.4 Ruang Lingkup

Pelaksanaan studi ini membatasi pengetahuan dan materi pembelajaran yang diteliti agar lebih terfokus dan atas dasar keterbatasan waktu dan tempat. Ruang lingkup subjek masalah dibatasi pada analisis risiko bahaya *cyber crime identity theft* dan pengendalian risiko bahaya berupa *cyber security* pada Personel AAL dengan batasan objek populasi beberapa orang Taruna dan anggota tetap di lingkungan Akademi TNI Angkatan Laut.

1.5 Sistematika

a. Bab I Pendahuluan.

Bab I Pendahuluan berisi tentang latar belakang permasalahan yang terjadi, dilanjutkan dengan perumusan masalah, menentukan tujuan dan manfaat, ruang lingkup penelitian, sistematika, serta membuat daftar pengertian.

b. Bab II Tinjauan Pustaka

Bab II Tinjauan Pustaka berisi tentang uraian peneliti dalam tinjauan pustaka berupa penelitian terdahulu, serta teori-teori yang relevan untuk dijadikan pisau analisis.

c. Bab III Metodologi Penelitian

Bab III Metodologi Penelitian berisi tentang metode penelitian, populasi dan sampel penelitian, instrumen penelitian, teknik pengumpulan dan pengolahan data, teknik analisis data dan tahapan penelitian.

d. Bab IV Pembahasan

Bab IV Pembahasan berisi tentang deskripsi hasil penelitian, hasil pengujian dan pembahasan hasil penelitian.

e. Bab V Penutup

Bab V Penutup berisi tentang sajian peneliti mengenai kesimpulan dan saran terhadap penelitian yang telah dilakukan.

1.6 Daftar Pengertian

a. *Cyber Crime*

Cyber crime atau kejahatan siber merupakan tindak kejahatan yang dilakukan di dunia maya. *Cyber crime* yang telah terjadi di dunia maya

menimbulkan kasus - kasus yang merugikan dan berdampak negatif bagi korban. *Cyber crime* tidak hanya terjadi di Indonesia, tetapi juga mencakup seluruh dunia (Habibi & Liviani, 2020).

b. Manajemen Risiko

Manajemen risiko adalah proses organisasi dalam mengidentifikasi, menilai, dan mengendalikan berbagai ancaman dan tantangan terhadap pencapaian tujuan. Untuk mengurangi risiko maka rencana pengembangan manajemen risiko mencakup proses perusahaan untuk mengidentifikasi dan mengendalikan berbagai ancaman terhadap semua aspek (Sarjana, et al., 2020).

c. *Identity Theft*

Rebovich menyatakan bahwa *identity theft* atau pencurian identitas adalah tindakan menggunakan informasi pribadi milik orang lain tanpa persetujuan dari pemilik informasi asli seperti nomor jaminan sosial, nama, alamat, nomor telepon, nomor SIM atau informasi identitas lainnya untuk menyamarkan identitas mereka dan hal tersebut dapat menimbulkan berbagai kerugian (Mahmud, 2019).

d. Keamanan data

Keamanan data mengacu pada langkah-langkah perlindungan privasi digital yang diterapkan untuk mencegah akses tidak sah ke komputer database dan situs web (Silalahi, 2022).

e. *Cyber Security*

Cyber security (Keamanan Siber) merupakan suatu aktivitas dengan maksud untuk melindungi perangkat komputer, perangkat mobile, server, sistem elektronik, jaringan, dan data dari beraneka jenis serangan jahat digital (Silalahi, 2022).

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian–Penelitian Terdahulu

Dalam penulisan skripsi yang berjudulkan “ANALISIS MANAJEMEN RISIKO BAHAYA *CYBER CRIME IDENTITY THEFT* TERHADAP PERSONEL AKADEMI TNI ANGKATAN LAUT” terdapat beberapa penelitian terdahulu yang dijadikan bahan acuan oleh penulis, antara lain:

Tabel 2.1 Penelitian Terdahulu

NO	NAMA	JUDUL PENELITIAN	HASIL PENELITIAN	RELEVANSI	
				PERSAMAAN	PERBEDAAN
1	2	3	4	5	6
1	Ineu Rahmawati, 2017	Analisis Manajemen Risiko Ancaman Kejahatan Siber (*Cyber Crime*) Dalam Peningkatan *Cyber Defense.*	Risiko yang dihadapi dalam mengatasi ancaman kejahatan siber tidak kalah dengan perang konvensional. Hal ini menyebabkan risiko yang diidentifikasi harus bisa menghasilkan strategi pertahanan negara dalam menghadapi ancaman kejahatan siber.	Kedua penelitian sama - sama membahas mengenai manajemen risiko bahaya *cyber crime*.	Penelitian terdahulu membahas mengenai keseluruhan kejahatan siber, sedangkan penelitian yang kami lakukan hanya terfokus pada kejahatan siber pencurian identitas atau *cyber crime identity theft* dengan studi kasus di Akademi TNI

NO	NAMA	JUDUL PENELITIAN	HASIL PENELITIAN	RELEVANSI	
				PERSAMAAN	PERBEDAAN
1	2	3	4	5	6
			(Rahmawati, 2017)		Angkatan Laut.
2	Mohammad Haswin Al-Rafi, 2024	Analisis Angka *Cyber Crime Identity Theft* Guna Menumbuhkan Kesadaran *Cyber Security* Pada Taruna Akademi TNI Angkatan Laut.	Taruna Akademi TNI Angkatan Laut belum memiliki kesadaran *cyber security* yang kuat untuk dapat mengantisipasi perkembangan ancaman *cyber crime identity theft*.	Kedua penelitian sama - sama membahas mengenai *cyber crime identity theft*.	Perbedaaan dalam pengambilan sampel dan tujuan penelitian dimana penelitian ini bertujuan untuk menganalisis angka *cyber crime identity theft* sedangkan penelitian yang kami lakukan untuk menganalisis manajemen risiko *cyber crime identitiy theft*.
3	(Sufi, Putri, & Suhartini, 2023)	Analisis Ancaman *Cyber Crime* dan Peran Sistem	Peran biometrik muncul sebagai alternatif yang menarik dalam upaya	Kedua penelitian sama - sama membahas mengenai	Penelitian terdahulu membahasa mengenai penggunaan

NO	NAMA	JUDUL PENELITIAN	HASIL PENELITIAN	RELEVANSI	
				PERSAMAAN	PERBEDAAN
1	2	3	4	5	6
		Biometrik *Systematic Literature Review*.	melindungi keuangan dari *cyber crime*. Meskipun belum sepenuhnya sempurna, biometrik mampu mengurangi risiko dan melindungi data keuangan dari *cyber crime*.	ancaman bahaya *cyber crime* atau risiko guna mencari upaya melindungi atau tindak mitigasi.	biometrik dalam pencegahan *cyber crime.* Sedangkan penelitian kami membahas analisis risiko bahaya *Cyber crime identity theft* dan tindak mitigasi

Sumber : Diolah oleh Peneliti (2024)

2.2 Teori–Teori Relevan

a. Teori Manajemen Risiko

Manajemen risiko adalah proses mengenali, mengukur, dan mengelola risiko secara lebih transparan yang dilengkapi dengan alat, teknik, dan sains yang diperlukan. Tujuan manajemen risiko adalah meminimalisasi pengaruh yang tidak baik akibat yang tidak terduga, dengan cara menghindari risiko atau mempersiapkan rencana kontingensi yang berkaitan dengan risiko tersebut. Jadi secara umum, manajemen risiko dapat dikatakan sebagai proses mengidentifikasi, mengukur dan memastikan risiko dan mengembangkan strategi untuk mengelola risiko tersebut. Kunci yang perlu diperhatikan dalam manajemen risiko agar bisa efektif, yaitu mengidentifikasi, menganalisis dan menilai risiko sejak awal secara sistematis dan mengembangkan rencana untuk menanganinya (Fathoni, 2020).

Manajemen risiko adalah suatu bidang ilmu yang membahas tentang bagaimana suatu organisasi menerapkan ukuran dalam memetakan

berbagai permasalahan yang ada dengan menempatkan berbagai pendekatan manajemen secara komprehensif dan sistematis (Arta, et al., 2021). Manajemen risiko adalah proses organisasi dalam mengidentifikasi, menilai, dan mengendalikan berbagai ancaman dan tantangan terhadap pencapaian tujuan. Untuk mengurangi risiko maka rencana pengembangan manajemen risiko mencakup proses perusahaan untuk mengidentifikasi dan mengendalikan berbagai ancaman terhadap semua aspek (Sarjana, et al., Manajemen Risiko, 2022). Teori manajemen risiko ini digunakan sebagai teori utama untuk menjadi pisau analisis dalam menjawab persoalan bagaimana cara mengurangi risiko *cyber crime identity theft* bagi Personel Akademi TNI Angkatan Laut dengan mengidentifikasi risiko, menganalisis peringkat risiko dengan menilai kemungkinan dan keparahan risiko, sehingga diperoleh masukan berupa tindak mitigasi yang tepat untuk dapat menjawab persoalan tersebut.

Gambar 2.1 Matriks Peringkat Risiko

Sumber: (Cholil, Santoso, Syahrial, Sinulingga, & Nasution, 2020)

b. Teori *Cyber Crime*

Cyber crime merupakan bentuk-bentuk kejahatan yang timbul karena pemanfaatan teknologi internet. Beberapa pendapat mengidentifikasi *cyber crime* dengan *computer crime*. *The U.S. Department of Justice* memberikan pengertien *computer crime* sebagai: *"any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution"*. Pengertian tersebut identik dengan yang diberikan *Organization of European Community Development*, yang mendefinisikan *computer crime* sebagai:

“any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data”. Dalam dua dokumen Kongres PBB mengenai The *Prevention of Crime and the Treatment of Offenders di Havana*, Cuba pada tahun 1990 dan di Wina, Austria pada tahun 2000, ada dua istilah yang dikenal:

1) *Cyber crime* dalam arti sempit disebut *computer crime*, yaitu prilaku illegal atau melanggar secara langsung menyerang system keamanan suatu komputer atau data yang diproses oleh komputer
2) *Cyber crime* dalam arti luas disebut *computer related crime*, yaitu prilaku ilegal atau melanggar yang berkaitan dengan sistem komputer atau jaringan

Dari beberapa pengertian diatas, secara ringkas dapat dikatakan bahwa *cyber crime* dapat didefinisikan adalah suatu tindakan kriminal yang melanggar hukum dengan menggunakan teknologi komputer sebagai alat kejahatannya. *Cyber crime* ini terjadi karena ada kemajuan di bidang teknologi komputer atau media internet. Maraknya tindak kriminal di dunia maya tergantung dari sejauh mana sumber daya baik berupa *hardware/software* maupun pengguna teknologi yang bersangkutan mempunyai pengetahuan dan kesadaran tentang pentingnya keamanan di dunia maya, seorang penyedia layanan/target *Cyber crime* harus mempunyai pengetahuan yang cukup tentang metode yang biasanya seorang *cyber crime* lakukan dalam menjalankan aksinya.

Kejahatan *cyber crime* memiliki berbagai jenis kategori dalam setiap pelaksanaanya. Berikut bentuk kejahatan *cyber crime*: (Hidayatullah, 2023)

1) Peretasan

Peretasan adalah salah satu bentuk pelanggaran. Ini adalah penggunaan yang tidak sah, atau akses ke, komputer atau sumber daya jaringan, yang mengeksploitasi kerentanan keamanan yang teridentifikasi dalam jaringan. Peretasan dapat digunakan untuk mengumpulkan data atau informasi pribadi yang digunakan untuk penjahat merusak situs web.

2) Spam

Spam adalah email yang tidak diminta atau 'sampah', biasanya

dikirim secara massal ke penerima yang tak terhitung jumlahnya di seluruh dunia dan sering dikaitkan dengan produk farmasi atau pornografi.

3) Serangan semantik

Serangan semantik adalah modifikasi dan penyebaran informasi yang benar dan salah. Informasi yang dimodifikasi bisa saja dilakukan tanpa menggunakan komputer meski peluang baru bisa ditemukan dengan menggunakan komputer. Untuk mengatur seseorang ke arah yang salah atau untuk menutupi jejak Anda, penyebaran informasi yang salah dapat digunakan.

4) *Cyberattacks*

Cyberattacks atau Serangan cyber adalah jenis manuver ofensif yang digunakan oleh negara-negara, individu, kelompok, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer dan atau perangkat komputer pribadi dengan berbagai cara tindakan berbahaya yang biasanya berasal dari sumber anonim yang mencuri, mengubah atau menghancurkan target yang di tentukan dengan cara membobol sistem yang rentan.

5) *Cyberextortion*

Cyberextortion terjadi saat sebuah situs web, server e-mail atau sistem komputer dikenai atau diancam dengan penolakan berulang terhadap layanan atau serangan lainnya oleh hacker jahat. Para hacker ini menuntut uang sebagai imbalan dengan janji akan menghentikan serangannya dan atau menawarkan "perlindungan". Menurut Biro Investigasi Federal, saat ini semakin banyak serangan yang dilakukan para pelaku *cyberextortion* pada situs web perusahaan dan jaringan, melumpuhkan kemampuan / kinerja mereka untuk beroperasi dan menuntut pembayaran untuk memulihkan layanan mereka. Lebih dari 20 kasus dilaporkan setiap bulan ke FBI dan banyak yang tidak dilaporkan untuk menjaga agar nama korban tidak keluar dan tersebar ke publik.

6) *Cyberwarfare*

Departemen Pertahanan Amerika Serikat mencatat bahwa

dunia maya telah menjadi perhatian tingkat nasional melalui beberapa peristiwa terkini mengenai signifikansi geostrategis. Di antaranya termasuk serangan terhadap infrastruktur Estonia di tahun 2007, yang diduga oleh hacker Rusia. "Pada bulan Agustus 2008, Rusia kembali melakukan serangan *cyber,* kali ini dalam kampanye kinetik dan non kinetik yang terkoordinasi dan disinkron kan melawan negara Georgia. Khawatir bahwa serangan semacam itu dapat menjadi norma perang antar negara di masa depan, dampak dari konsep operasi dunia maya akan disesuaikan oleh para komandan militer di masa depan

7) Pencurian Data (*Identity Theft*)

Istilah yang digunakan untuk mendeskripsikan saat informasi disalin atau diambil secara ilegal dari bisnis atau individu lain. Umumnya, informasi ini adalah informasi pengguna seperti kata sandi, nomor jaminan sosial, informasi kartu kredit, informasi pribadi lainnya, atau informasi rahasia perusahaan lainnya. Karena informasi ini diperoleh secara tidak sah, ketika individu yang mencuri informasi ini ditangkap, kemungkinan besar akan dituntut secara hukum.

Cyber Crime merupakan akses illegal atau kejahatan dunia maya yang menggunakan computer sebagai sasaran atau objek utama dalam melakukan pencurian data jaringan (*Identity Theft*) dan pembobolan situs. Kejahatan yang menjadikan sistem teknologi informasi sebagai sarana pencurian data pribadi (*Identity Theft*) merupakan ancaman yang sangat berbahaya bagi institusi AAL.

c. Teori *Identity Theft*

Menurut USSA *Educational Fondation, Identity Theft* dapat didefinisikan sebagai pencurian identitas yang terjadi saat seseorang menggunakan nama, alamat, nomor Jaminan Sosial, bank atau kartu kredit nomor rekening atau informasi pribadi lainnya tanpa izin untuk melakukan penipuan atau kejahatan. Dapat disimpulkan bahwa pencurian identitas (*Identity Theft*) adalah tindakan pencurian data pribadi atau penggunaan data pribadi tanpa seizin orang yang bersangkutan untuk melakukan penipuan atau kegiatan ilegal. Hal ini bisa berupa nama, nomor identitas, nomor kartu kredit, informasi akun bank nomor asuransi dan lainnya. Seseorang yang

melakukan tindakan tersebut biasanya digunakan untuk keuntungan pribadi sehingga hal ini bisa menyebabkan kerugian baik materil maupun non-materil. Di era yang sangat berkembang pesat ini terutama tentang teknologi dan informasi angka kejahatan dalam pencurian identitas (*identity theft*) tentunya sangatlah tinggi.

Pentingnya kesadaran masyarakat dalam menjaga informasi identitas mereka juga perlu ditekankan karena pencurian identitas dapat melalui berbagai macam jalur dan cara. Laporan yang dikeluarkan oleh (The University of Texas at Austin, 2017) mengatakan bahwa terdapat beberapa jalur pendistribusian yang melibatkan orang luar dan orang dalam. Dampak kerugian yang tercatat pada tahun 2017 mengatakan untuk kasus *magnetic stripe* sebesar $28,909,617, atm pin $24,223,391, *fake id card information* $15,117,824, *financial information* $13,722,781, dan *age information* $11,977,044 yang terjadi di amerika.

Kejahatan pencurian identitas adalah jenis kejahatan yang memiliki berbagai jenis kategori dalam setiap pamanfaatanya. (Identity Theft Resource Center, 2018) membagi 5 kategori pencurian identitas yaitu sebagai berikut:

1) Criminal Identity Theft

Criminal identity theft adalah ketika seorang penjahat secara ilegal mengidentifikasi diri mereka ke polisi atau petugas sebagai individu lain. Dalam beberapa kasus, penjahat sebelumnya memperoleh dokumen identitas yang dikeluarkan negara menggunakan kredensial (pengesahan dari pihak ke-3) yang dicuri dari orang lain, atau hanya menunjukkan ID palsu. Disini korban kemungkinan besar dapat terjerat kasus yang serius. Berikut ini adalah contoh dari simulasi *criminal identity theft*:

a) Pelaku melakukan sebuah tindakan kriminal.

b) Pelaku menggunakan identitas palsu dan berpura - pura sebagai orang lain (korban).

c) Dakwaan dikirim ke korban.

d) Pelaku bersih dari pelanggaran yang dialakukan.

2) Financial Identity Theft

Financial identity theft yaitu di mana seseorang ingin mendapatkan manfaat ekonomis atas nama orang lain. Ini termasuk mendapatkan kredit, pinjaman, dana atau barang dan jasa. Dalam garis besaranya adalah pencurian identitas financial untuk mendapatkan keutungan materi dari identitas orang yang dicuri. Berikut ini adalah contoh dari simulasi *financial identity theft*:

a) Pelaku melakukan sebuah transaksi / penarikan.

b) Pelaku menggunakan identitas palsu (kartu kredit atau identitas lainnya).

c) Tagihan / pemberitahuan dibebankan kepada korban.

d) Pelaku menikmati hasil.

3) Identity Cloning

Dalam situasi ini pencuri identitas menyamar sebagai orang lain untuk menyembunyikan identitas mereka yang sebenarnya. Biasanya untuk mendapatkan beberapa keutungan dari cloning identitas tersebut. Contohnya seperti poster, label yang diberikan kepada orang yang menggunakan foto dan informasi orang lain di situs jejaring sosial. Berikut ini adalah contoh dari simulasi *identity cloning*:

a) Pelaku melakukan cloning identitas.

b) Pelaku menggunakan identitas palsu (foto, aktivitas, nama, tanggal lahir, dan informasi lainnya).

c) Pelaku mendapatkan keutungan dengan cara mengaku–ngaku.

d) Pelaku menikmati hasil.

4) Medical Identity Theft

Peneliti privasi Pam Dixon, pendiri World Privacy Forum, yang dirilis pertama kali tahun 2006. Pencurian identitas medis terjadi ketika seseorang mencari perawatan medis di bawah identitas orang lain. Pencurian asuransi juga sangat umum, jika pencuri memiliki informasi asuransi korban dan atau kartu asuransi, maka mereka dapat mencari perhatian medis seolah–olah seperti korban itu sendiri. Berikut ini

adalah contoh dari simulasi *medical identity theft*:

a) Pelaku melakukan klaim kesehatan.

b) Pelaku menggunakan identitas palsu (nama, tanggal lahir, nomor kebijakan, kode diagnosis, nomor jaminan sosial).

c) Tagihan dan diagnosa dikirim ke korban.

d) Pelaku tidak terkena tagihan.

5) Child Identity Theft

Child identity theft atau pencurian identitas anak terjadi ketika identitas anak di bawah umur digunakan oleh orang lain untuk keuntungan pribadi si penipu. Si penipu dapat berupa anggota keluarga, teman, atau bahkan orang asing yang menargetkan anak - anak. Jumlah Jaminan Sosial anak dihargai karena mereka tidak memiliki informasi yang terkait dengan mereka. Pencuri dapat membuat jalur kredit, mendapatkan SIM, atau bahkan membeli rumah menggunakan identitas anak. Penipuan ini dapat tidak terdeteksi selama bertahun-tahun, karena sebagian besar anak-anak tidak menemukan masalah sampai bertahun-tahun kemudian disaat mereka beranjak dewasa & diharuskan untuk mengurusi dan melengkapi kewajiban mereka sebagai warga negara seperti SIM, KTP dan mungkin kartu asuransi. Berikut ini adalah contoh dari simulasi *child identity theft*:

a) Pelaku mencuri identitas anak.

b) Pelaku menggunakan identitas palsu (nama, tanggal lahir, kartu jaminan sosial, dan informasi lainnya).

c) Tagihan / pemberitahuan dibebankan ke korban.

d) Pelaku menikmati hasil.

Banyaknya kejahatan dari pencurian data serta dampaknya yang sangat besar dalam segala aspek di kehidupan seseorang, maka banyak ahli yang mengemukakan teori - teori dan pendapatnya untuk memberikan pemahaman dan kesadaran penggunaan teknologi. Oleh karena itu, Teori mengenai pencurian data atau *identity theft* ini dapat dijadikan bahan analisis untuk dilakukan analisis terhadap risiko terjadinya yang akan menghasilkan tindak mitigasi guna mengurangi risiko tersebut bagi Personel AAL.

BAB III
METODE PENELITIAN

3.1 Metode Penelitian

Metode penelitian pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Metode penelitian yang digunakan bersifat deskriptif dengan pendekatan kuantitatif (Sugiyono, 2018). Penelitian deskriptif adalah penelitian yang menggunakan observasi, wawancara atau angket mengenai keadaan sekarang ini, mengenai subjek yang sedang kita teliti. Melalui angket dan sebagainya kita mengumpulkan data untuk menguji hipotensis atau menjawab suatu pertanyaan (Ruseffendi, 2010).

Pendekatan penelitian yang digunakan yaitu penelitian kuantitatif, metode penelitian kuantitatif diartikan sebagai metode penelitian yang berlandaskan pada filsafat positivisme, digunakan untuk meneliti pada populasi atau sampel tertentu, pengumpulan data menggunakan instrumen penelitian, analisis data bersifat kuantitatif/statistik, dengan tujuan untuk mengacu hipotensis yang telah ditetapkan. Pendekatan kuantitatif ini digunakan peneliti untuk menganalisis fenomena (Sugiyono, 2018).

Penelitian ini dilakukan dengan pendekatan *HIRADC (Hazard Identification Risk Assessment and Determining Control)* yaitu proses mengidentifikasi bahaya, mengukur, dan mengevaluasi risiko yang muncul dari sebuah bahaya dalam suatu organisasi, untuk selanjutnya dilakukan penilaian risiko dari bahaya tersebut. Hasil dari penilaian risiko tersebut berguna untuk membuat program pengendalian bahaya agar meminimalisir tingkat risiko yang mungkin terjadi sehingga dapat mencegah terjadinya bahaya (Cholil, et al., 2020). Metode ini diambil berdasarkan pada tujuan dari penelitian ini yaitu mengidentifikasi risiko bahaya *cyber crime identity theft*, menganalisis tingkatan risiko bahaya *cyber crime identity theft* dan membuat tindak mitigasi yang dilakukan terhadap risiko bahaya tertinggi *cyber crime identity theft*. Mengacu pada metode ini, maka pelaksanaan penelitian ini melalui studi kasus yang merupakan kombinasi dari pengamatan, pengumpulan data dan analisisnya untuk memperoleh gambaran menyeluruh terkait “Analisis Manajemen Risiko Bahaya *Cyber Crime Identity Theft* Terhadap Personel Akademi TNI Angkatan Laut”.

3.2 Fokus Penelitian

Fokus dari penelitian ini berdasarkan pada judul dan metode yang telah ditetapkan yaitu mengarah pada analisis manajemen risiko bahaya *cyber crime identity theft* terhadap Personel Akademi TNI Angkatan Laut, dengan beberapa pokok bahasan untuk dapat menjawab persoalan sebagai berikut:

a. Seberapa besar nilai bahaya *cyber crime identity theft* terhadap Personel Akademi TNI Angkatan Laut?

b. Bagaimana tindak mitigasi yang dilakukan untuk mengurangi risiko bahaya *cyber crime identity theft* pada Personel Akademi TNI Angkatan Laut?

3.3 Sumber dan Jenis Data

Sumber dan jenis data dalam penelitian ini sesuai dengan pokok bahasan terkait manajemen risiko bahaya *cyber crime identity theft* pada Personel Akademi TNI Angkatan Laut. Sumber data diperoleh dari berbagai narasumber di beberapa tempat untuk mendapatkan berbagai data primer dan data sekunder yang diperlukan sebagai bahan analisis tingkatan risiko bahaya *cyber crime identity theft* terhadap Personel Akademi TNI Angkatan Laut.

a. Sumber Data.

Pada dasarnya sumber data merupakan subyek ataupun tempat untuk mendapatkan dan mengumpulkan data sesuai dengan fokus penelitian. Sumber data merupakan asal didapatkannya sebuah data atau sekelompok data. Selain itu dikatakan pula bahwa sumber data merupakan subjek dari mana data dapat diperoleh (Arikunto, 2013). Berdasarkan pemahaman tersebut, maka sumber data dalam penelitian kuantitatif ini merupakan data campuran dari sumber studi pustaka baik media cetak maupun media elektronik dengan hasil wawancara dari narasumber serta hasil dari observasi penulis di lingkungan tempat penelitian.

Sumber Data diperoleh dari Populasi yang bersifat heterogen/homogen mengingat objek penelitian merupakan narasumber/subyek yang memberikan masukan dan pandangannya terkait pokok bahasan/objek yang dibahas menyangkut analisis manajemen risiko bahaya *Cyber Crime Identity Theft* terhadap personel Akademi TNI Angkatan

Laut, dalam hal ini adalah para ahli/pakar di bidang siber dan beberapa taruna sebagai sumber data untuk mendapatkan tingkatan risiko dari bahaya *cyber crime identity theft* di lingkungan Akademi TNI Angkatan Laut.

b. Jenis Data

1) Data Primer

Data primer merupakan data yang didapat dari penulis atau dari nara sumber baik secara individu maupun secara kelompok terkait peringkat risiko bahaya *cyber crime identity theft* terhadap Personel Akademi TNI Angkatan Laut dengan menggunakan metode observasi dan wawancara. Observasi dilaksanakan di lingkungan Akademi TNI Angkatan Laut. Sedangkan metode wawancara dilaksanakan kepada para ahli atau narasumber yang terkait nilai kemungkinan (*likehood*) dan nilai dampak (*severity*) variabel risiko bahaya berdasarkan standar AS/NZS 4360.

2) Data Sekunder

Data sekunder merupakan data yang tidak didapat langsung oleh penulis atau didapat menggunakan pihak perantara. Data ini merupakan data yang diperoleh dari berbagai media cetak maupun media elektronik, serta data informasi dari pihak-pihak lain terkait dengan penelitian yang sedang diteliti oleh penulis.

3.4 Instrumen Penelitian

Penelitian ini akan menggunakan metode observasi dan wawancara dalam pengumpulan data primer, serta melalui studi pustaka dalam pengumpulan data sekunder. Observasi dilakukan dengan memperhatikan gambaran kondisi lingkungan sekitar serta pengalaman para Personel Akademi TNI Angkatan Laut mengenai *cyber crime identity theft*. Pada metode wawancara dilaksanakan secara terarah dan wawancara secara mendalam, baik dengan persiapan daftar pertanyaan maupun langsung sesuai kondisional narasumber yang terkait. Untuk mendukung hal tersebut, maka ada beberapa instrumen penelitian yang digunakan, yaitu:

a. Media Elektronika.

Instrumen media elektronika yang digunakan dalam penelitian ini

berupa alat perekam, kamera, laptop serta handphone untuk mendukung dokumentasi data penelitian observasi dan hasil wawancara terhadap narasumber.

b. Kertas Dokumen

Instrumen dokumentasi dalam bentuk lembaran yang digunakan dalam penelitian ini berupa daftar pertanyaan dan hasil wawancara sebagai sumber data otentik untuk diolah dan dianalisis.

3.5 Teknik Pengumpulan Data

Teknik pengumpulan data ialah langkah yang paling strategis dalam penelitian, dikarenakan tujuan dari penelitian ialah mencari data yang relevan dan valid (Sugiyono, 2015). Pengumpulan data dengan menggunakan metode penelitian kuantitatif menggunakan instrumen pengumpulan data berupa observasi dan wawancara serta studi pustaka dengan keterangan:

a. Observasi

Yaitu mengadakan pengamatan langsung terhadap obyek penelitian secara terbatas serta pengalaman penugasan Peneliti selama melakukan pendidikan kedinasan untuk mendapatkan gambaran yang umum terhadap masalah angka *cyber crime identity theft* dan bahaya *cyber security* pada personel Akademi TNI Angkatan Laut.

b. Wawancara

Yaitu mengadakan wawancara melalui interview dan dialog langsung dengan para nara sumber yang dipakai sebagai subyek untuk memberikan data terkait objek penelitian dengan berpedoman pada daftar pertanyaan yang telah disusun. Kegiatan ini dilakukan melalui tatap muka langsung maupun media daring secara kondisional, serta berbagai diskusi dan sharing yang intensif dengan memanfaatkan waktu dan media komunikasi yang ada.

c. Studi Pustaka

Di samping observasi maupun wawancara dan kuesioner, teknik pengumpulan data dilakukan melalui studi kepustakaan yang merupakan pengumpulan data melalui literatur yang berupa buku, catatan, dan laporan penelitian dari riset yang dilakukan sebelumnya, baik data internal seperti dokumen resmi maupun data eksternal dari buku, jurnal, artikel dan dari

media internet.

3.6 Pengelolahan Data

Pengelolahan data ialah proses atau Langkah penelitian selanjutnya setelah data dikumpulkan dengan tujuan menyaring, menganalisis, menilai dan meberikan hasil yang didapatkan. Langkah ini guna memastikan dan menyusun informasi dari data yang diperoleh telah sesuai dan valid dengan tujuan dari penelitian. Dalam pengelolahan data, peneliti menggunakan metode penelitian kuantitatif dengan analisis HIRADC untuk mendapatkan hasil yang diharapakan untuk risiko bahaya *cyber crime identity* theft terhadap personel akademi TNI Angkatan laut.

3.7 Teknik Analisis Data

Data yang telah terkumpul dalam tahap pengumpulan data, perlu diolah terlebih dahulu. Pengolahan data tersebut bertujuan untuk lebih menyederhanakan semua data yang terkumpul dan menyajikannya dalam susunan yang baik, rapi kemudian dianalisis.

Analisis yang dilakukan penelitian yang penulis rencanakan adalah sebagai berikut:

a. Identifikasi Risiko

Identifikasi risiko dilakukan dengan observasi dan wawancara. Observasi atau pengamatan secara langsung dilakukan di lingkungan Akademi TNI Angkatan Laut serta wawancara dilakukan terhadap korban beberapa Personel Akademi TNI Angkatan Laut yang pernah mengalami kasus *cyber crime identity theft* untuk mendapatkan variabel risiko bahaya *cyber crime identity theft*. Variabel yang telah didapatkan kelak akan diukur nilai kemungkinan dan dampaknya agar dapat dilakukan pengendalian terhadap risiko bahaya tersebut sesuai dengan peringkat risikonya.

b. Analisis Risiko

Analisis risiko berisi penilaian terhadap variabel risiko bahaya yang telah didapatkan pada identifikasi risiko. Responden atau sampel melakukan penilaian risiko (*risk assessment*) yang berpedoman pada *Australia Standard/ New Zealand Standard* (AS/NZS 4360) agar dapat diketahui nilai risiko dari segi seberapa sering terjadinya (*likehood)* dan besarnya kerugian

risiko tersebut (*severity*).

Tabel 3.1 Ukuran dari "likelihood”

Level	***Likehood***	**Uraian**
1	*Rare*	Jarang terjadi (risiko terjadi sekali dalam waktu >5 tahun)
2	*Unlikely*	Cenderung dapat terjadi di suatu waktu (risik dapat terjadi sekali antara 1 – 5 tahun)
3	*Possible*	Bisa terjadi di suatu waktu (Risiko mungkin terjadi 1-6 kali setahun)
4	*Likely*	Kemungkinan akan terjadi di banyak situasi (Risiko mungkin terjadi rata-rata 1 kali setiap bulan)
5	*Almost Certain*	Hampir pasti terjadi dan akan terjadi di semua situasi (Risiko terjadi minimum seminggu 1 kali)

Sumber :Guruh Prasetyo Putro, S.ST., M.Si (Han)(2022)

Tabel 3.2 Ukuran dari "severity”

Level	***Severity***	**Uraian**
1	*Insignificant*	Tanpa kerugian materi (tidak menimbulkan kerugian berarti)
2	*Minor*	Kerugian materi kecil (mengganggu pekerjaan maksimum 4 jam atau kemungkinan kerugiannya Rp.100.000 – Rp.300.000)
3	*Moderate*	Kerugian materi cukup besar (mengganggu pekerjaan maksimum 24 jam atau kemungkinan kerugiannya Rp.300.000 – Rp.1.000.000)
4	*Major*	Kerugian materi besar hingga pekerjaan terhambat (mengganggu pekerjaan maksimum 3x24 jam atau kemungkinan

Level	*Severity*	Uraian
		kerugiannya Rp.1.000.000 – Rp.3.000.000)
5	*Extreme*	Kerugian materi sangat besar dan dampak luas (mengganggu pekerjaan lebih dari 3x24 jam atau kemungkinan kerugiannya > Rp.3.000.000)

Sumber :Guruh Prasetyo Putro, S.ST., M.Si (Han)(2022)

Setelah dilakukannya penilaian risiko dan didapatkan nilai dari kedua kriteria yaitu *likehood* dan *severity*, dilakukan pemeringkatan risiko mendapatkan nilai peringkat dari masing - masing risiko bahaya berdasarkan standar AS/NZS 4360.

Peringkat risiko = Kemungkinan (*likehood*) x Dampak (*severity*).

Dari nilai indeks risiko yang telah didapatkan, dilakukan penetapan peringkat risiko (*risk level*). Kelompok peringkat risiko dibagi menjadi empat yaitu *Extreme* (E), *High* (H), *Moderate* (M), dan *Low* (L).

Tabel 3.3 Matriks Peringkat Risiko Menurut Standar AS/NZS 4360

Matriks Peringkat Risiko			***Severity***				
			1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Extreme*
Likehood	5	*Almost Certain*	**M**	**H**	**H**	**E**	**E**
	4	*Likely*	**M**	**M**	**H**	**H**	**E**
	3	*Possible*	**L**	**M**	**H**	**H**	**H**
	2	*Unlikely*	**L**	**L**	**M**	**M**	**H**
	1	*Rare*	**L**	**L**	**M**	**M**	**H**

Sumber : AS/NZS 4360: *Risk Management (1990)*

Keterangan :

L (*low*) = risiko rendah

M (*moderate*)= risiko sedang

H (*high*) = risiko tinggi

E (e*xtreme*) = risiko ekstrim

c. Tindak Mitigasi Risiko

Tindak mitigasi risiko dilakukan setelah mengelompokkan risiko berdasarkan rankingnya (*risk level*), dimana:

1) Tingkat risiko menengah (*moderate*) - ekstrim (*extreme*) termasuk risiko yang significant atau risiko dengan tingkat bahaya yang perlu dilakukan pengendalian risiko sesuai hierarki pengendalian risiko.

2) Tingkat risiko rendah adalah risiko yang dapat diterima atau tidak significant namun risiko ini harus tetap dimonitor. (Alijoyo, Wijaya, & Jacob, 2021).

Tindak mitigasi risiko dilakukan dengan tujuan untuk meminimalisir risiko bahaya *cyber crime identity theft* di Akademi TNI Angkatan Laut. Tindak mitigasi yang dilakukan berupa memberikan langkah – langkah penerapan *cyber security* terhadap variabel risiko terkait yang berisiko tinggi. Tindak mitigasi dalam penelitian ini dilakukan dengan studi literatur dan juga wawancara lanjutan dengan sampel expert di bidang *cyber security* guna memvalidasi apakah data mengenai tindak mitigasi valid dan dapat diterapkan di Akademi Angkatan Laut.

3.8 Tahap Kegiatan Penelitian

Tabel 3.4 Tahap Kegiatan Penelitian

NO.	KEGIATAN	WAKTU
1.	Pengajuan judul ke prodi	Minggu ke-I bulan September 2024
2.	Paparan judul skripsi di tingkat prodi	Minggu ke-II bulan September 2024
3.	Pembuatan proposal	Minggu ke-II bulan Oktober – minggu ke-II bulan November 2024
4.	Ujian proposal	Minggu ke-II bulan Desember 2024
5.	Penelitian dan penyelesaian skripsi	Minggu ke-IV bulan Desember 2024 – minggu ke-V bulan April 2025
6.	Ujian skripsi	Minggu ke-IV bulan Mei 2025
7.	Revisi	Minggu ke-IV bulan Mei 2025

Sumber : diolah oleh peneliti (2024)

BAB IV
PEMBAHASAN

4.1 Deskripsi Penelitian

Dalam penelitian ini, peneliti mengkorelasikan seluruh aspek yang digunakan dalam penelitian ini antara lain : rumusan masalah, identifikasi masalah, data dukung maupun pelaksanaan penelitian yang ditujukan untuk menyelesaikan masalah dengan urgensi yang relevan dengan permasalahan yang bertajuk pada fenomena internasional yang terealisasikan di lingkungan TNI-AL, dibahas khusus di penelitian kami di akademi angkatan laut, yang dimana *identity theft* ini dapat terjadi kapan saja dan dimana saja di lingkungan social kita, yang pada pelaksanaan penugasan maupun kegiatan sehari-hari bersinggungan dengan teknologi maupun media sosial.

Akademi TNI Angkatan Laut merupakan Lembaga Pendidikan pertama perwira yang berdiri di bawah tanggung jawab dan wewenang dari Akademi TNI, yang bertugas mencetak perwira lulusan akademi yang handal, unggul dan professional di dalam melaksanakan tugasnya. Perwira yang dibentuk dari instansi ini tentu harus memiliki identitas yang bersih baik secara perbuatan maupun dari segi administratif, yang membuat mereka menjadi rentan terhadap pelanggaran yang disebabkan baik dari pihak mereka sendiri maupun dari pihak yan tidak berwenang. Perwira lulusan dari AAL tentu sudah dibekali oleh Lembaga terhadap bagaimana berkehidupan menjadi perwira yang bersih dari perbuatan yang tercela, hanya saja dari perspektif penaggulangan terhadap ancaman berupa pengeksploitasian data oleh pihak yang tidak berwenang belum ada dan dilaksanakan oleh lembaga, dimana hal ini menjadi memiliki urgensi yang tinggi mengingat hal-hal yang terjadi secara global menjadi sangat masih terhadap kehidupan seluruh manusia dan tidak mengecualikan manusia yang memiliki profesi sebagai tantara. Oleh karena itu, penulis memiliki inisiasi untuk melaksanakan penelitian ini sebagai salah satu saran penyaluran saran sekaligus pertimbangan bagi otoritas akademi yang berwenang dalam mempertimbangkan mitigasi yang serius terhadap probabilitas ancaman yang ada.

Pada fokus penelitian ini, peneliti akan menekankan dan berfokus terhadap kasus-kasus pelanggaran *cyber* yang umunya terjadi di Akademi TNI Angkatan Laut, seperti : eksploitasi data oleh pihak yang tidak bertanggung jawab, *Pishing*

yang dilaksanakan secara massif, maupun peretasan yang terjadi dikarenakan kerentanan system *cyber security*, maupun pelanggaran *cyber* lain yang umum terjadi di Akademi TNI Angkatan Laut yang memiliki dampak yang signifikan terhadap eksistensi dari instansi.

Penelitian ini dilaksanakan dengan metode kuantitatif, dimana penelitian ini dilaksanakan secara linear dengan hasil pengkolektifan data yang dilaksanakan menggunakan wawancara. Setalah hasil wawancara di dapatkan, maka peneliti akan mengimplementasikan hasil wawancara di dalam pengolahan data dengan menggunakan metode HIRADC. Metode HIRADC dipilih karena merupakan metode yang melibatkan salah satu unsur penting dalam penyelesaian masalah, yaitu *risk assessment* dimana *risk assessment* ini menjadi salah satu mindset dalam metode penyelesaian masalah yang mengkalkulasi masalah dengan akurat dan memberikan mitigasi yang terukur terkait dengan masalah yang dihadapinya. Dengan metode HIRADC ini kalukulasi terhadap kasus yang sifatnya berupa *identity theft* dapat dilaksanakan dengan baik.

a. Data Primer

Data primer merupakan data yang didapat dari penulis atau dari nara sumber baik secara individu maupun secara kelompok terkait angka bahaya *cyber crime identity theft* pada Akademi TNI Angkatan Laut dengan menggunakan metode wawancara, kuesioner dan observasi. Metode wawancara dilaksanakan kepada para ahli atau narasumber yang terkait Analisis Angka *Cyber Crime Identity Theft* khususnya di lingkungan Akademi TNI Angkatan Laut maupun dengan nara sumber lain umumnya melalui saluran komunikasi yang ada. Adapun data primer yang didapatkan dari beberapa responden dengan beberapa variabel risiko yang telah dikelompokkan dan di identifikasi kemungkinan besar dapat terjadi di Akademi Angkatan Laut. Berikut daftar tabel variabel risiko yang telah dibuat untuk melaksanakan penelitian

Tabel 4.1 Potensi Bahaya dan Variabel Resiki Kecelakaan

No	Potensi bahaya	Variabel Risiko Kecelakaan
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada (Observasi)

No	Potensi bahaya	Variabel Risiko Kecelakaan
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting (Observasi)
		3. Malware dapat merusak jaringan komputer (Observasi)
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban (Observasi)
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax (Observasi)
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku (Observasi)
		4. Tabungan dikuras setelah masuk ke situs palsu (Observasi)
		5. Mengambil data internal untuk dibocorkan ke publik (Observasi)
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin (Observasi)
		2. Kerugian materiil dengan nominal yang cukup besar (Observasi)
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena *Cracking* sehingga menghambat pekerjaan (Observasi)
		2. Terjadinya deface atau perubahan tampilan pada *system* (Observasi)
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress (Observasi)
		2. Pemerasan terhadapn korban dengan

No	Potensi bahaya	Variabel Risiko Kecelakaan
		ancaman (Observasi)
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual (Observasi)

Sumber : Diolah oleh Peneliti (2025)

1) Penilaian risiko terhadap Likehood (Kemungkinan)

Penilaian likehood (kemungkinan) dilakukan agar dapat mendapat nilai likehood untuk setiap variabel. Setiap variabel berkemungkinan memiliki nilai likehood yang berbeda sehingga perhitungannya dilakukan masing-masing setiap item. Penilaian likehood dilakukan kepada 3 narasumber sebagai Kadispamsanal, Kasubdis Inteltek dan Kasi Analevsifor Satsiber Dispamsanal

a) Penilaian Likehood (Kemungkinan) Risiko menurut Kadispamsanal.

Hasil survey likehood setiap item variabel risiko dari salah satu responden yaitu responden yang berposisi sebagai Kadispamsanal di Mabesal

Tabel 4.2 Survey Likehood

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada		√			
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting		√			
		3. Malware dapat merusak jaringan komputer			√		

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban			√		
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax			√		
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku		√			
		4. Tabungan dikuras setelah masuk ke situs palsu			√		
		5. Mengambil data internal untuk dibocorkan ke publik		√			
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin			√		
		2. Kerugian materi dengan nominal yang cukup besar			√		
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan		√			
		2. Terjadinya deface atau perubahan tampilan pada sistem		√			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			√		
		2. Pemerasan terhadap korban dengan ancaman			√		

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual		√			

Sumber : Diolah oleh Peneliti (2025)

b) Penilaian Likehood (Kemungkinan) Risiko Menurut Kasubdisinteltek.

Hasil survey likehood setiap item variabel risiko dari salah satu responden yaitu responden yang berposisi sebagai Kasubdis Inteltek di Dispamsanal.

Tabel 4.3 Tabel Survey Likehood

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada			√		
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	√				
		3. Malware dapat merusak jaringan komputer		√			
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban				√	
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax			√		

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku		√			
		4. Tabungan dikuras setelah masuk ke situs palsu				√	
		5. Mengambil data internal untuk dibocorkan ke publik		√			
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				√	
		2. Kerugian materi dengan nominal yang cukup besar			√		
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan		√			
		2. Terjadinya deface atau perubahan tampilan pada sistem		√			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			√		
		2. Pemerasan terhadap korban dengan ancaman				√	
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual		√			

Sumber : Diolah oleh Peneliti (2025)

c) Penilaian Likehood (Kemungkinan) Risiko Menurut Narasumber 3

Hasil survey likehood setiap item variabel risiko dari salah satu responden yang berposisi sebagai Kasi Analevsifor Satsiber Dispamsanal.

Tabel 4.4 Survey Likehood

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada			√		
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting			√		
		3. Malware dapat merusak jaringan komputer			√		
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban			√		
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				√	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku		√			
		4. Tabungan dikuras setelah masuk ke situs palsu			√		
		5. Mengambil data internal untuk dibocorkan ke publik				√	

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				√	
		2. Kerugian materi dengan nominal yang cukup besar			√		
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan		√			
		2. Terjadinya deface atau perubahan tampilan pada sistem		√			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			√		
		2. Pemerasan terhadap korban dengan ancaman				√	
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual		√			

Sumber : Diolah oleh Peneliti (2025)

2) Penilaian Risiko Terhadap Severity (Keparahan)

Penilaian severity (keparahan) dilakukan agar mendapat nilai severity untuk setiap variabel. Setiap variabel berkemungkinan memiliki nilai severity yang berbeda sehingga perhitungannya dilakukan masing-masing setiap item. Penilaian severity dilakukan kepada 3 narasumber yang berposisi sebagai Kadispamsanal, Kasubdis Inteltek dan Kasi Analevsifor Satsiber Dispamsanal.

a) Penilaian severity (Keparahan) risiko menurut

Kadispamsanal

Hasil survey severity setiap item variabel risiko dari salah satu responden yaitu responden yang berposisi sebagai Kadispamsanal

Tabel 4.5 Survey Severity

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada					√
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting		√			
		3. Malware dapat merusak jaringan komputer				√	
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban					√
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				√	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku			√		
		4. Tabungan dikuras setelah masuk ke situs palsu					√
		5. Mengambil data internal untuk dibocorkan ke publik				√	
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				√	

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
		2. Kerugian materi dengan nominal yang cukup besar					√
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan			√		
		2. Terjadinya deface atau perubahan tampilan pada sistem		√			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			√		
		2. Pemerasan terhadap korban dengan ancaman					√
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual				√	

Sumber : Diolah oleh Peneliti (2025)

b) Penilaian Severity (Keparahan) Risiko Menurut Kasubdis Inteltek

Hasil survey severity setiap item variable risiko dari salah satu responden yaitu responden yang berposisi sebagai Kasubdisinteltek di Mabesal

Tabel 4.6 Survey Severity

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada					√

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting		√			
		3. Malware dapat merusak jaringan komputer					√
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban				√	
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				√	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku			√		
		4. Tabungan dikuras setelah masuk ke situs palsu					√
		5. Mengambil data internal untuk dibocorkan ke publik			√		
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				√	
		2. Kerugian materi dengan nominal yang cukup besar					√
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan			√		
		2. Terjadinya deface atau perubahan tampilan pada sistem		√			

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress				√	
		2. Pemerasan terhadap korban dengan ancaman					√
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual			√		

Sumber : Diolah oleh Peneliti (2025)

c) Penilaian Severity (Keparahan) Risiko Menurut Koordinator narasumber 3

Hasil survey severity setiap item variable risiko dari salah satu responden yaitu responden yang berposisi sebagai Kasi Analevsifor Satsiber Dispamsanal

Tabel 4.7 Survey Severity

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada				√	
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	√				
		3. Malware dapat merusak jaringan komputer			√		
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban					√

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				√	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku				√	
		4. Tabungan dikuras setelah masuk ke situs palsu				√	
		5. Mengambil data internal untuk dibocorkan ke publik		√			
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin					√
		2. Kerugian materi dengan nominal yang cukup besar					√
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan				√	
		2. Terjadinya deface atau perubahan tampilan pada sistem		√			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			√		
		2. Pemerasan terhadap korban dengan ancaman					√
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual				√	

Sumber : Diolah oleh Peneliti (2025)

b. Data Sekunder

Pengumpulan data sekunder dilakukan melalui metode wawancara dan diskusi dengan nara sumber yang kompeten berkaitan dengan Bahaya Cyber Crime, serta berbagai bentuk peluang dan ancaman terkait perkembangan dari Bahaya *Cyber Crime Identity Theft* di Lingkungan Akademi TNI Angkatan Laut. Berdasarkan hasil wawancara yang diperoleh peneliti kepada seluruh Narasumber, pola yang digunakan oleh pelaku dari tahun- ketahun selalu berbeda namun tetap dengan tujuan yang sama. Pola yang sangat sering dilakukan adalah

1) Malware

Malware adalah perangkat lunak berbahaya yang diprogram untuk merusak atau untuk mendapatkan akses ke sistem komputer tanpa sepengetahuan pemilik sistem (Zalavadiya & Priyanka, 2017).

Berupa virus, trojan, worm dan jenis jenis *software* lainnya. Virus merupakan jenis *software* yang dapat merusak dan mengubah data dari korban. Trojan adalah *software* yang Dimana meniru/menyamar sebagai *software* yang sah namun melakukan aktivitas yang berbahaya. Selanjutnya adalah *Worm* merupakan *software* yang menggandakan dirinya sendiri dan dapat menyebabkan kerusakan ekstensif.

2) Phising

Menurut Sutan Remy Syahdeni *Phising* adalah pengiriman *e-mail* palsu kepada orang tahu suatu perusahan dengan menyatakan bahwa pengirim adalah suatu entitas bisnis yang sah untuk memperoleh informasi pribadi dari korbannya (2009) Pelaku mengirimkan pesan yang berupa *file*, *file* tersebut adalah *Malware* yang dimana *Malware* ini dapat menjadi jembatan bagi pelaku siber untuk mengetahui data- data apa saja yang ada didalam *device user*, data yang sangat bisa diambil adalah data transaksi keuangan, data *m-banking*, data pesan masuk dan keluar di berbagai aplikasi, data *file* yang ada di dalam *device*, data panggilan masuk dan keluar dan bahkan data percapakan *user* pun tak luput dari aksi pelaku. *Phishing* adalah Tindakan kejahatan yang memancing *user* dengan cara

mengirimkan *file* yang berisi *Malware* ke *e- mail*, *website* dan komunikasi elektronik lainnya. *Phishing* hanya dapat digunakan jika *user* memiliki jaringan internet (*Online)*. Kenapa *user* sering kali terjebak dengan tindakan kejahatan *phishing* ini, adalah karena kelalaian dan minim informasi akan bahaya *cyber crime*. *User* cenderung menggunakan *gadget* hanya untuk komunikasi dan hiburan semata, seiring berjalannya waktu, pelaku *phishing* sudah sangat mempersiapkan bagaimana pesan tersebut dapat terlihat seperti pesan yang sungguhan dan sering kali pesan tersebut diiringi atau berisi ajakan, ancaman dan pemberitahuan.

3) Skimming

Skimming adalah tindakan untuk mengambil intisari atau saripati dari suatu hal. Artinya dalam membaca cepat dengan melihat dan memperhatikan bahan bacaan untuk mencari ide pokok dari suatu bacaan (Soedarso, 2010).

Skimming merupakan suatu kasus yang dikarenakan *user* itu sendiri, contohnya Ketika *user* hendak melakukan transaksi di ATM (Anjungan Tunai Mandiri), *user* yang teliti pasti akan melakukan pengecekan terlebih dahulu terhadap mesin ATM. Apakah di mesin tersebut ada yang janggal, contoh, Ketika hendak memasukkan kartu di mesin ATM, jika *user* teliti. *Skimming* merupakan tindakan pencurian data kartu ATM/Debit dengan cara menyalin, membaca dan menyimpan informasi yang terdapat di strip magnetis secara illegal. Strip magnetis itu terletak pada bagian belakang kartu ATM/Debit berupa garis hitam, garis hitam ini berisi data nasabah, nomor kartu, masa berlaku kartu. Jika pelaku melancarkan aksinya di mesin ATM/Debit, alat *Skimmin*g ini diletakkan pada slot kartu ketika user hendak melakukan transaksi, *Skimming* ini juga bisa dilakukan pada mesin EDC pembayaran. *Skimming* di mesin ATM, juga didukung oleh pelaku dengan meletakkan kamera kecil tersembunyi yang bertujuan untuk mengetahui PIN dari *user* dan ada juga yang mengintip secara langsung. Jika pelaku sudah mendapatkan semua data yang diperlukan, mereka membuat kartu baru untuk melakukan transaksi.

4) Cracking

Cracking merupakan suatu kegiatan merusak sistem yang bertujuan untuk kepentingan pribadi dengan cara yang tidak sah (Anthoni, 2018). Kegiatan ini terjadi bilamana pelaku sudah mentargetkan korban sebagai “bahan/tujuan” yang mereka lakukan. *Cracking* tidak dapat dihindari oleh siapapun dan kapanpun bisa terjadi.

5) Bullying

UNICEF menjelaskan *cyberbullying* (perundungan dunia maya) ialah bullying atau perundungan dengan menggunakan teknologi digital. Hal ini dapat terjadi di media sosial, platform chatting, platform bermain game, dan ponsel. *Cyberbullying* merupakan perilaku berulang yang ditunjukan untuk menakuti, membuat marah, atau mempermalukan mereka yang jadi sasaran. *Bullying* secara langsung atau tatap muka dan *cyberbullying* seringkali dapat terjadi secara bersamaan. Namun, *cyberbullying* meninggalkan jejak digital atau sebuah rekaman yang dapat berguna dan memberikan bukti ketika membantu menghentikan perilaku salah ini. (Fitria Aulia, 2021)

Untuk saat ini, kita dihadapkan pada era globalisasi dan era digitalisasi secara luas, dimana kita dapat mengakses internet tanpa batas dan dapat memilih perangkat yang diinginkan sebagai sarana untuk mengakses informasi dari manapun dan kapanpun. Hal yang paling dasar untuk mengantisipasi kejahatan siber adalah tingkatkan kesadaran akan bahaya kejahatan siber, selalu waspada dan teliti jika menerima *file* dari yang tidak di kenal (*e-mail*, aplikasi perpesanan), jika itu belum cukup maka harus mengetahui dasar-dasar ilmu dari teknologi dan informasi yang berkaitan dengan bahaya *cyber crime*.

Terkait pembekalan pengetahuan kepada prajurit dan Taruna untuk menumbuhkan kesadaran bahaya dari *cyber crime* adalah setiap prajurit dan taruna harus memiliki kesadaran dan kewaspadaan terkait kejahatan ini, jika seseorang tidak berhati-hati dengan kejahatan ini, pasti akan menjadi hal yang merugikan dikemudian harinya. Untuk mengatasi dan mencegah terjadinya ancaman dari bahaya *cyber crime* maka prajurit dan taruna harus

memahami tentang *Cyber Security*. *Cyber Security* adalah salah satu keamanan yang saat ini harus menjadi tanggung jawab masing-masing, namun pembekalan di institusi dan meningkatkan kesadaran adalah hal yang paling penting dilakukan. Mungkin tidak semua orang dapat memilki keahlian atau keterampilan di *cyber security*, namun dengan adanya edukasi dan tingginya tingkat kesadaran akan pentingnya *cyber security*, menjadikan ruang gerak pelaku kejahatan ini menjadi sempit.

4.2 Analisis Data

Fokus dari penelitian ini berdasarkan pada judul dan metode yang telah ditetapkan yaitu mengarah pada Analisis Manajemen Risiko Bahaya *Cyber Crime Identity Theft* terhadap Personel Akademi TNI Angkatan laut, serta tindak mitigasi yang tepat untuk mengurangi risiko bahaya *cyber crime identity theft* terhadap Personel Akademi TNI Angkatan laut tersebut. Dalam hal ini peneliti menggunakan Analisis Peringkat Risiko yang mengacu pada Matriks Indeks Risiko berdasarkan standar AS/NZS 4360 sebagai pisau analisis untuk mengolah data penelitian.

Evaluasi risiko dilakukan dengan menghitung perkalian dari nilai *likehood* (kemungkinan) dan *severity* (keparahan). Misalkan variabel risiko memiliki nilai serevity (4) dan nilai probabilty (3), maka variabel tersebut tergolong peringkat H - *High* (risiko Tinggi). (Mengacu Pada Tabel 3.3 Matriks Peringkat Risiko Menurut Standar AS/NZS 4360)

Matriks Indeks Risiko berdasarkan AS/NZS 4360 menjelaskan bahwa terdapat variabel berada pada daerah warna hijau dengan kode L - *Low* (Rendah), terdapat variabel pada daerah kuning dengan kode M - *Moderat*e (Sedang), terdapat variabel pada daerah merah dengan kode H – *High* (Tinggi) serta pada daerah merah tua terdapat kode E - *Extreme* (Ekstrim).

a. Peringkat Risiko Menurut Narasumber 1

Hasil peringkat atau *ranking* risiko menurut Narasumber 1 yang datanya telah diolah oleh penulis hingga didapatkan peringkat risiko dari masing - masing variabel, dapat ditentukan bahwa:

1) Variabel dengan kategori L-*Low* (rendah) yaitu sebanyak 2 variabel.

2) Variabel dengan kategori M-*Moderate* (sedang) yaitu sebanyak

4 variabel

3) Variabel dengan kategori H-*High* (tinggi) yaitu sebanyak 9 variabel.

4) Variabel dengan kategori E-*Extreme* (ekstrim) yaitu sebanyak 0 variabel / tidak ada.

Hasil peringkat risiko tertera pada Tabel 4.8 Peringkat Risiko menurut Narasumber 1.

Tabel 4.8 Peringkat Risiko menurut Narasumber 1.

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*	*Severity*	Peringkat Risiko
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada	2	5	H
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	2	2	L
		3. Malware dapat merusak jaringan komputer	3	4	H
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban	3	5	H
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax	3	4	H
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku	2	3	M
		4. Tabungan dikuras setelah masuk ke situs palsu	3	5	H
		5. Mengambil data internal untuk dibocorkan ke publik	2	4	M

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*	*Severity*	Peringkat Risiko
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin	3	4	H
		2. Kerugian materi dengan nominal yang cukup besar	3	5	H
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan	2	3	M
		2. Terjadinya deface atau perubahan tampilan pada sistem	2	2	L
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress	3	3	H
		2. Pemerasan terhadap korban dengan ancaman	3	5	H
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual	2	4	M

Sumber : diolah oleh peneliti (2025)

b. Peringkat Risiko Menurut Narasumber 2

Hasil peringkat atau *ranking* risiko menurut Narasumber 2 yang datanya telah diolah oleh penulis hingga didapatkan peringkat risiko dari masing - masing variabel, dapat ditentukan bahwa:

1) Variabel dengan kategori L-*Low* (rendah) yaitu sebanyak 2 variabel.

2) Variabel dengan kategori M-*Moderate* (sedang) yaitu sebanyak 4 variabel

3) Variabel dengan kategori H-*High* (tinggi) yaitu sebanyak 8 variabel.

4) Variabel dengan kategori E-*Extreme* (ekstrim) yaitu sebanyak 1 variabel / tidak ada.

Hasil peringkat risiko tertera pada Tabel 4.9 Peringkat Risiko menurut Narasumber 2.

Tabel 4.9 Peringkat Risiko menurut Narasumber 2.

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*	*Severity*	Peringkat Risiko
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada	3	5	H
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	1	2	L
		3. Malware dapat merusak jaringan komputer	2	5	H
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban	4	4	H
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax	3	4	H
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku	2	3	M
		4. Tabungan dikuras setelah masuk ke situs palsu	4	5	E
		5. Mengambil data internal untuk dibocorkan ke publik	2	3	M

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*	*Severity*	Peringkat Risiko
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin	4	4	H
		2. Kerugian materi dengan nominal yang cukup besar	3	5	H
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan	2	3	M
		2. Terjadinya deface atau perubahan tampilan pada sistem	2	2	L
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress	3	4	H
		2. Pemerasan terhadap korban dengan ancaman	4	5	H
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual	2	3	M

Sumber : diolah oleh peneliti (2025)

c. Peringkat Risiko Menurut Narasumber 3

Hasil peringkat atau *ranking* risiko menurut Narasumber 3 yang datanya telah diolah oleh penulis hingga didapatkan peringkat risiko dari masing - masing variabel, dapat ditentukan bahwa:

1) Variabel dengan kategori L-*Low* (rendah) yaitu sebanyak 2 variabel.

2) Variabel dengan kategori M-*Moderate* (sedang) yaitu sebanyak 4 variabel

3) Variabel dengan kategori H-*High* (tinggi) yaitu sebanyak 7

variabel.

4) Variabel dengan kategori E-*Extreme* (ekstrim) yaitu sebanyak 2 variabel / tidak ada.

Hasil peringkat risiko tertera pada Tabel 4.10 Peringkat Risiko menurut Narasumber 3.

Tabel 4.10 Peringkat Risiko menurut Narasumber 3.

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*	*Severity*	Peringkat Risiko
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada	3	4	H
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	3	1	L
		3. Malware dapat merusak jaringan komputer	3	3	H
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban	3	5	H
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax	4	4	H
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku	2	4	M
		4. Tabungan dikuras setelah masuk ke situs palsu	3	4	H
		5. Mengambil data internal untuk dibocorkan ke publik	4	2	M
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin	4	5	E

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*	*Severity*	Peringkat Risiko
		2. Kerugian materi dengan nominal yang cukup besar	3	5	H
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan	2	4	M
		2. Terjadinya deface atau perubahan tampilan pada sistem	2	2	L
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress	3	3	H
		2. Pemerasan terhadap korban dengan ancaman	4	5	E
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual	2	4	M

Sumber : diolah oleh peneliti (2025)

d. Rekapitulasi Peringkat Risiko

Hasil peringkat risiko menurut ketiga narasumber diolah ke dalam satu tabel agar terlihat perbedaan dan persamaan peringkat risiko pada masing - masing variabel risiko yang tertera pada Tabel 4.11 Rekapitulasi Peringkat Risiko.

Tabel 4.11 Rekapitulasi Peringkat Risiko.

No	Potensi bahaya	Risiko Kecelakaan	*Narasumber 1*	*Narasumber 2*	*Narasumber 3*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada	H	H	H
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	L	L	L
		3. Malware dapat merusak jaringan komputer	H	H	H
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban	H	H	H
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax	H	H	H
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku	M	M	M
		4. Tabungan dikuras setelah masuk ke situs palsu	H	E	H
		5. Mengambil data internal untuk dibocorkan ke publik	M	M	M
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin	H	H	E
		2. Kerugian materi dengan nominal yang cukup besar	H	H	H

No	Potensi bahaya	Risiko Kecelakaan	*Narasumber 1*	*Narasumber 2*	*Narasumber 3*
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan	M	M	M
		2. Terjadinya deface atau perubahan tampilan pada sistem	L	L	L
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress	H	H	H
		2. Pemerasan terhadap korban dengan ancaman	H	H	E
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual	M	M	M

Sumber : Diolah oleh Peneliti (2025)

Secara keseluruhan, peringkat risiko setiap variabel yang dijawab oleh ketiga responden cenderung sama. Hal ini dikarenakan tugas utama dan fokus masing – masing responden yang memiliki keterkaitan. Ketiga responden berada di dalam bidang yang sama yakni bidang Cyber dengan gambaran tugas utama dari masing - masing responden yaitu:

1) Narasumber 1 : Laksamana Pertama Bambang Suseno Indro Pranoto S.H,CHRPM., M.Tr.Opsla dengan jabatan / posisi Kadispamsanal (Kepala Dinas Persandian Angkatan Laut) memiliki tugas utama untuk mengelola seluruh kegiatan persandian di lingkungan TNI Angkatan Laut. Tugas-tugasnya meliputi penyusunan rencana dan program, inventarisasi dan evaluasi kebutuhan peralatan sandi, serta perencanaan dan distribusi peralatan tersebut.

2) Narasumber 2 : Kolonel Laut (E) Muhammad Bashori Alwi, S.T.,M.T. dengan jabatan / posisi Kasubdis Inteltek (Kepala Subdinas

Intelijen dan Teknologi) memiliki peran strategis dalam struktur organisasi yang menggabungkan fungsi intelijen dan teknologi di TNI Angkatan Laut. Kasubdis Inteltek bertanggung jawab untuk mengintegrasikan fungsi intelijen dan teknologi guna mendukung kebijakan dan keputusan strategis melalui pengumpulan, analisis, dan pemanfaatan informasi serta teknologi secara efektif dan efisien.

3) Narasumber 3: Letkol (E) Risman dengan jabatan / posisi Kasi Analevsifor Dispamsanal (Kepala Seksi Analisis Evaluasi dan Penyusunan Strategi) memiliki peran strategis dalam membangun strategi yang dapat digunakan untuk mencegah ancaman *cyber crime* pada TNI Angkatan laut. Kasi Analevsifor bertugas dan bertanggung jawab atas rencana atau strategi yang harus disiapkan guna melawan serangan *cyber crime.*

4.3 Tindak Mitigasi Risiko

Tindak mitigasi risiko merupakan tahapan akhir dalam manajemen risiko. Mitigasi risiko dilakukan setelah didapatkan peringkat dari masing-masing variabel risiko.

Cara untuk menentukan apakah variabel risiko tersebut perlu dilakukan mitigasi adalah melihat peringkat risiko dari hasil penilaian responden. Variabel risiko yang memerlukan tindak mitigasi adalah variabel yang memiliki peringkat risiko E-*Extreme* (ekstrim), H-*High* (tinggi), atau M-*Moderate* (sedang) dari minimal 1 responden. Apabila ketiga responden memiliki hasil penilaian sama terhadap salah satu variabel risiko dan peringkat risikonya L-*Low* (rendah) maka variabel risiko tersebut tidak perlu dilakukan tindak mitigasi namun harus tetap dimonitor.

Maka dari cara diatas, variabel yang perlu tindakan mitigasi diantaranya:

a. Malware

1) Variabel Risiko Bahaya

a) Malware dapat mencuri data-data perangkat dan informasi yang ada

b) Malware dapat merusak jaringan computer

2) Tindak Mitigasi

Tindak mitigasi dapat meliputi penggunaan perangkat lunak keamanan, pembaruan sistem dan aplikasi, serta kewaspadaan terhadap tautan dan lampiran mencurigakan.

Deteksi melibatkan pemindaian rutin dan komprehensif menggunakan perangkat lunak antivirus dan anti-malware. Respons terhadap serangan melibatkan tindakan seperti mematikan sistem, melakukan pemulihan data, dan melaporkan insiden ke pihak berwenang.

b. Phising

1) Variabel Risiko Bahaya

a) Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban

b) Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax

c) Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku

d) Tabungan dikuras setelah masuk ke situs palsu

e) Mengambil data internal untuk dibocorkan ke publik

2) Tindak Mitigasi

a) Tingkatkan kesadaran akan keamanan dalam beraktivitas di ruang siber.

b) Tidak memberikan informasi yang berkenaan dengan data-data pribadi di media sosial karena dapat disalahgunakan oleh pihak yang tidak bertanggung jawab.

c) Tidak membagikan informasi sensitif kepada siapapun, seperti *username*, PIN, *password, One Time Password* (OTP) dan sebagainya.

d) Berhati-hatilah terhadap pihak yang mengaku berasal dari otoritas berwenang, namun meminta data-data sensitive.

e) Berhati-hati terhadap suatu link atau tautan yang mencurigakan atau tidak dikenal untuk menghindari diri dari serangan phishing.

c. Skimming

1) Variabel Risiko Bahaya

a) Terjadinya pencurian informasi pribadi seperti *username, password,* dan pin

b) Kerugian materi dengan nominal yang cukup besar

2) Tindak Mitigasi

Pencegahan meliputi memeriksa mesin ATM dan EDC sebelum digunakan, melindungi data kartu pribadi, dan mengganti PIN secara berkala. Penanganan meliputi segera melaporkan ke bank jika curiga terkena skimming dan mengganti kartu.

a) Pencegahan Skimming

Periksa Mesin ATM dan EDC, Perhatikan apakah ada bagian yang menonjol, longgar, atau mencurigakan di area slot kartu, Pastikan tidak ada alat yang terpasang di sekitar keypad atau slot kartu. Jika ada, jangan gunakan mesin tersebut dan laporkan ke bank.

b) Lindungi Data Kartu

Jangan sembarangan membagikan nomor kartu, CVV, dan tanggal kadaluwarsa. Gunakan metode pembayaran tanpa kartu (cardless payment) jika tersedia.

c) Ganti PIN Secara Berkala

Ganti PIN secara berkala untuk mengurangi risiko skimming atau bahkan jika PIN sudah sempat terekam, Hindari penggunaan PIN yang mudah ditebak seperti tanggal lahir, Pilih Lokasi ATM yang aman, Hindari mesin ATM di lokasi terpencil atau tanpa pengawasan, Pilih mesin ATM yang berada di lokasi ramai dan diawasi CCTV, Lakukan Transaksi dengan Hati-hati, Perhatikan sekeliling Anda saat memasukkan kartu dan PIN, Jangan biarkan orang lain melihat saat Anda memasukkan PIN.

d) Penanganan Jika Curiga Terkena Skimming

Segera hubungi bank dan laporkan kejadian, blokir kartu ATM Anda, ata ganti kartu ATM dengan kartu baru.

e) Lakukan Pemantauan Transaksi

Periksa riwayat transaksi secara berkala untuk mendeteksi transaksi mencurigakan, jika perlu melakukan transaksi sementara kartu lama diblokir, gunakan kartu debit atau kredit tambahan, dan laporkan ke Polisi

d. Cracking

1) Variabel Risiko Bahaya

Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan

2) Tindak Mitigasi

a) Memblokir akses yang tidak sah ke sistem atau jaringan komputer.

b) Perangkat Lunak Anti-Malware Mendeteksi dan menghapus perangkat lunak berbahaya yang dapat digunakan untuk cracking.

c) Peningkatan Keamanan Sistem operasi, aplikasi, dan perangkat keras dari potensi serangan cracking, misalnya dengan menggunakan password yang kuat dan kompleks.

3) Pencegahan Umum

Penggunaan Teknologi yang aman seperti VPN, untuk melindungi data dan privasi.

e. Bullying

1) Variabel Risiko Bahaya

a) Pelaku mengintimidasi korban hingga membuat stress

b) Pemerasan terhadap korban dengan ancaman

c) Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelcehan seksual

2) Tindak Mitigasi

a) Peningkatan Kesadaran dan Edukasi

Penting untuk memberikan edukasi tentang *cyberbullying*, dampaknya, dan cara mencegahnya kepada semua orang, terutama anak-anak dan remaja.

b) Etika Digital dan Penggunaan yang Bijaksana

Menumbuhkan kesadaran akan etika digital dan penggunaan media sosial yang bertanggung jawab dapat membantu mencegah perilaku cyberbullying.

c) Pengawasan Online

Taruna Akademi TNI Angkatan Laut perlu dipantau penggunaan sosial medianya, dan juga diberikan arahan dalam penggunaannya.

d) Budaya Online Positif

Mendorong budaya online yang positif, di mana orang saling menghormati dan menghargai, dapat membantu mengurangi risiko *cyberbullying*.

e) Menyediakan dukungan bagi korban

Penyediaan dukungan psikologis dan layanan konsultasi bagi korban *cyberbullying* sangat penting untuk membantu mereka mengatasi dampak trauma dan menyembuhkan.

f) Penyelesaian Kasus atau Pemberian Hukuman terhadap Pelaku

Pihak berwenang dapat menindak pelaku *cyberbullying* sesuai dengan hukum yang berlaku agar memberi efek jera dan juga mengurangi risiko terjadinya *cyberbullying.*

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian terkait analisis risiko bahaya *cyber crime identity theft* pada Personel Akademi TNI Angkatan Laut yang telah dijabarkan, terdapat hal penting yang perlu digaris bawahi berkaitan dengan perkembangan ancaman *cyber crime identity theft* yang sangat tinggi dan berdampak besar terhadap kerugian material maupun non-material, bahkan kerugian ini dapat bersifat fatal apabila menyangkut kehidupan sosial maupun kehidupan berbangsa dan bernegara yang lebih luas, seperti penyalahgunaan data oleh organisasi teroris atau separatis untuk menghancurkan bangsa dan negara Indonesia. Melalui metode penelitian kuantitatif dengan *tool analysis HIRADC* maka dapat ditarik kesimpulan sebagai berikut :

a. Penguatan sarana pengamanan *cyber* dengan membangun infrastruktur teknologi yang modern baik alat peralatan yang digunakan maupun kemudahan akses layanan dan jaringan yang kuat. Sehingga sistem pengamanannya pun akan semakin kuat untuk mencegah bahaya dari ancaman *cyber crime.*

b. Peningkatan pengetahuan tentang *cyber crime identity theft* terhadap personel Akademi TNI Angkatan Laut dengan memberikan sosialisasi bagaimana pengaman diri dari bahaya ancaman *cyber crime* sehingga timbulnya kesadaran dari bahaya *cyber crime.*

c. Penguatan sistem pengamanan *cyber* melalui pengembangan software maupun hardware yang modern dengan memiliki sistem keamanan yang kuat, pengetatan aturan-aturan terkait akses terhadap data pribadi sehingga informasi tidak mudah di akses oleh orang lain untuk mencegah terjadinya serangan *cyber crime.*

d. Meningkatkan progam pembinaan dan penguatan *cyber security* kepada personel Akademi TNI Angkatan Laut sehingga menumbuhkan kesadaran terhadap pentingnya keamanan dari bahaya *cyber crime.*

5.2 Saran

Sesuai tujuan dan manfaat dari penelitian ini yaitu untuk memberikan masukan bagi seluruh pemangku kebijakan dan *stakeholder* terkait angka *cyber*

crime identity theft, serta tindak mitigasi untuk mengurangi angka risiko *cyber* pada Personel Akademi TNI Angkatan Laut dalam menghadapinya, maka dapat disampaikan saran rekomendasi sebagai berikut:

a. Bagi Pemerintah diharapkan dapat memperkuat aturan dan kebijakan terhadap pengetatan akses data pribadi pengguna layanan siber yang digunakan oleh penyedia jasa sistem, meningkatkan infrastruktur pengamanan siber, sekaligus selalu mensosialisasikan pentingnya manajemen risiko guna mengurangi angka risiko bahaya *cyber crime identity theft* kepada seluruh Masyarakat.

b. Bagi Lembaga-lembaga pengamanan siber yang ada di Indonesia diharapkan dapat meningkatkan perannya dalam menjaga keamanan siber, serta mengadakan berbagai program pembinaan kesadaran *cyber security* kepada seluruh masyarakat secara intensif dan berkesinambungan.

c. Bagi Lembaga Pendidikan khususnya Akademi TNI Angkatan Laut diharapkan dapat meningkatkan pengetahuan peserta didik dengan memperkuat muatan Kurikulum Pelajaran siber yang lebih banyak, lebih komprehensif, serta dukungan alokasi waktu pembelajaran yang lebih lama dan didukung oleh tenaga pendidik yang kompeten.

d. Bagi Para Taruna Akademi TNI Angkatan Laut diharapkan dapat memperkuat manajemen risiko guna mengurangi angka risiko bahaya *cyber crime identity theft* melalui pembelajaran, literasi digital, serta memperkuat pengamanan gadget/akses digital dengan sandi dan deteksi fisik.

DAFTAR PUSTAKA

Ahmad, A. (2012). Perkembangan Teknologi Komunikasi dan Informasi: Akar Revolusi dan Berbagai Standarnya. *Jurnal Dakwah Tabligh, Vol. 13, No. 1*, 137-149.

Alijoyo, A., Wijaya, B., & Jacob, I. (2021). *Layers of Protection Analysis (Analisis Lapisan Proteksi).* Bandung: CRMS Indonesia.

Altheide, D. L. (1987). Ethnographic Analysis Content. *Qualitative Sociology*, 65-77.

Aminestia, T. D., & Prasetyono, P. N. (2023). Identifikasi Risiko Kecelakaan Kerja Pada Proyek Pembangunan Gedung Rumah Salkit Siti Khodijah Sidoarjo. *ViTeks Volume 1 No. 1*, 59-65.

Anton, T. J. (1979). *Occupational Safety Management And Engineering Fourth Edition.* New Jersey: Prentice Hall.

Arikunto. (2013). *Prosedur Penelitian Suatu Pendekatan Praktik. Edisi Revisi.* Jakarta: PT. Rineka Cipta.

Arta, I. P., Satriawan, D. G., Bagiana, I. K., Loppies, Y., Shavab, F. A., Mala, C. M., . . . Rustan, B. (2021). *Manajemen Risiko Tinjauan Teori dan Praktis.* Bandung: Widina Bhakti Persada.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2022). Retrieved from Survei Profil Internet Indonesia 2022.

Cholil, A. A., Santoso, S., Syahrial, T. R., Sinulingga, E. C., & Nasution, R. H. (2020). Penerapan Metode HIRADC Sebagai Upaya Pencegahan Risiko Kecelakaan Kerja Pada Divisi Operasi Pembangkit Listrik Tenaga Gas Uap. *Jurnal Bisnis & Manajemen*, 41-64.

Cholil, Azhar, A., Santoso, Sugeng, Syahrial, T., Sinulingga, C., & H, N. (2020). PENERAPAN METODE HIRADC SEBAGAI UPAYA PENCEGAHAN RISIKO KECELAKAAN KERJA PADA DIVISI OPERASI PEMBANGKIT LISTRIK TENAGA GAS UAP. *Jurnal Bisnis & Manajemen Vol.20 No.2*, 41-64.

Fathoni, M. Z. (2020). Analisis Risiko Pada Proyek Pembuatan Lintel Set Point Dengan Metode Kualitatif (Studi Kasus : PT. XYZ). *Jurnal Penelitian dan Aplikasi Sistem & Teknik Industri (PASTI)*, 113-126.

Gusti, R. N., & Wiguna, P. A. (2021). Analisis Risiko Kecelakaan Kerja pada Proyek Pembangunan Gedung Kampus II UINSA Surabaya. *Jurnal Teknik ITS Vol.*

10, No. 2, 2337-3539.

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Jurnal Pemikiran dan Pembaharuan Hukum Islam*, 401-426.

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cyber Security di Indonesia; Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen Vol.5*, 1-17.

Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Sains dan Teknologi Vol.2 No.1*, 216-221.

Identity Theft Resource Center. (2018). Retrieved from https://www.idtheftcenter.org/

Mahmud, R. (2019). Pencurian Identitas Kategori & Kasus. *CyberSecurity dan Forensik Digital, Vol. 2, No. 1*, 39-42.

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara* , 51-66.

Ruseffendi, E. T. (2010). *Dasar-Dasar Penelitian Pendidikan dan Bidang Non Eksakta Lainnya.* Bandung: Tarsito.

Sarjana, S., Nardo, R., Hartono, R., Siregar, Z. H., Irmal, Sohilauw, M. I., . . . Badrianto, Y. (2020). Bandung: CV. MEDIA SAINS INDONESIA.

Sarjana, S., Nardo, R., Hartono, R., Siregar, Z. H., Irmal, Sohilauw, M. I., . . . Badrianto, Y. (2022). *Manajemen Risiko.* Bandung: Media Sains Indonesia.

Silalahi, F. D. (2022). *Keamanan Siber (Cyber Security).* Semarang: Yayasan Prima Agus Teknik.

Sufi, F. Y., Putri, D. K., & Suhartini, D. (2023). Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review. *Seminar Nasional Akuntansi*, 19-22.

Sugiyono. (2015). *Metode penelitian Kombinasi (Mix Methods).* Bandung: Alfabeta.

Sugiyono. (2018). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D.* Bandung: Alfabeta.

The University of Texas at Austin. (2017). *Identity Theft Assessment and Prediction Report.*

LAMPIRAN

Lampiran 1 Formulir Wawancara

TUJUAN SURVEY

Agar dapat mengetahui nilai dari segi kemungkinan terjadinya risiko bahaya *(likehood)* dan tingkat keparahan atau dampak dari kemungkinan risiko *(severity)*. Sehingga dapat menjadi acuan dalam menentukan peringkat risiko bahaya cyber crime identity theft yang ada di lingkungan Akademi Angkatan Laut.

PROFIL RESPONDEN

Nama :
Telepon :
Jabatan / Posisi :

PETUNJUK PENGISIAN KUISIONER

Berilah dan isilah penilaian pada tabel yang diberi angka berdasarkan standar Standar AS/NZS 4360 dengan persepsi terhadap kemungkinan terjadinya risiko *(likehood)* dan besarnya kerugian (*severity*) apabila risiko bahaya tersebut terjadi, aspek keuangan, SDM, Sdan lain-lain.

Level	***Likehood***	**Uraian**
1	*Rare*	Jarang terjadi (risiko terjadi sekali dalam waktu >5 tahun)
2	*Unlikely*	Cenderung dapat terjadi di suatu waktu (risik dapat terjadi sekali antara 1 – 5 tahun)
3	*Possible*	Bisa terjadi di suatu waktu (Risiko mungkin terjadi 1-6 kali setahun)
4	*Likely*	Kemungkinan akan terjadi di banyak situasi (Risiko mungkin terjadi rata-rata 1 kali setiap bulan)
5	*Almost Certain*	Hampir pasti terjadi dan akan terjadi di semua situasi (Risiko terjadi minimum

Level	***Likehood***	**Uraian**
		seminggu 1 kali)

Sumber :Guruh Prasetyo Putro, S.ST., M.Si (Han)(2022)

Level	***Severity***	**Uraian**
1	*Insignificant*	Tanpa kerugian materi (tidak menimbulkan kerugian berarti)
2	*Minor*	Kerugian materi kecil (mengganggu pekerjaan maksimum 4 jam atau kemungkinan kerugiannya Rp.100.000 – Rp.300.000)
3	*Moderate*	Kerugian materi cukup besar (mengganggu pekerjaan maksimum 24 jam atau kemungkinan kerugiannya Rp.300.000 – Rp.1.000.000)
4	*Major*	Kerugian materi besar hingga pekerjaan terhambat (mengganggu pekerjaan maksimum 3x24 jam atau kemungkinan kerugiannya Rp.1.000.000 – Rp.3.000.000)
5	*Extreme*	Kerugian materi sangat besar dan dampak luas (mengganggu pekerjaan lebih dari 3x24 jam atau kemungkinan kerugiannya > Rp.3.000.000)

Sumber :Guruh Prasetyo Putro, S.ST., M.Si (Han)(2022)

No	Potensi Bahaya	Variabel Risiko Kecelakaan	Penilaian Risiko									
			Severity					*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*	*Level 1*	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada										
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting										
		3. Malware dapat merusak jaringan komputer										
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban										
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax										
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku										
		4. Tabungan dikuras setelah masuk ke situs palsu										
		5. Mengambil data internal untuk dibocorkan ke publik										

No	Potensi Bahaya	Variabel Risiko Kecelakaan	Penilaian Risiko									
			Severity					*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*	*Level 1*	*Level 2*	*Level 3*	*Level 4*	*Level 5*
3		informasi pribadi seperti username password dan pin										
		2. Kerugian materiil dengan nominal yang cukup besar										
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan										
		2. Terjadinya deface atau perubahan tampilan pada sistem										
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress										
		2. Pemerasan terhadap korban dengan ancaman										
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual										

Lampiran 2 Hasil Wawancara Narasumber 1

PROFIL RESPONDEN

Nama : Laksamana Pertama Bambang Suseno Indro Pranoto S.H,CHRPM., M.Tr.Opsla

Telepon : -

Jabatan / Posisi : Kadispamsanal (Kepala Dinas Persandian Angkatan Laut)

a) Hasil Wawancara Nilai *Likehood*

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada		✓			
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting		✓			
		3. Malware dapat merusak jaringan komputer			✓		
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban			✓		
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax			✓		
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku		✓			
		4. Tabungan dikuras setelah masuk ke situs palsu			✓		
		5. Mengambil data internal untuk dibocorkan ke publik		✓			

3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin			✓		
		2. Kerugian materi dengan nominal yang cukup besar			✓		
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan		✓			
		2. Terjadinya deface atau perubahan tampilan pada sistem		✓			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			✓		
		2. Pemerasan terhadap korban dengan ancaman			✓		
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual		✓			

b) Hasil Wawancara Nilai *Severity*

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada					✓
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting		✓			

		3. Malware dapat merusak jaringan komputer				✓	
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban					✓
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				✓	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku			✓		
		4. Tabungan dikuras setelah masuk ke situs palsu					✓
		5. Mengambil data internal untuk dibocorkan ke publik				✓	
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				✓	
		2. Kerugian materi dengan nominal yang cukup besar					✓
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan			✓		
		2. Terjadinya deface atau perubahan tampilan pada sistem		✓			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			✓		
		2. Pemerasan terhadap korban dengan ancaman					✓

		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual				✓	

Lampiran 3 Hasil Wawancara Narasumber 2

PROFIL RESPONDEN

Nama : Kolonel Laut (E) Muhammad Bashori Alwi, S.T.,M.T.

Telepon : -

Jabatan / Posisi : Kasubdis Inteltek

a) Hasil Wawancara Nilai *Likehood*

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada			✓		
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	✓				
		3. Malware dapat merusak jaringan komputer		✓			
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban				✓	
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax			✓		
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku		✓			
		4. Tabungan dikuras setelah masuk ke situs palsu				✓	
		5. Mengambil data internal untuk dibocorkan ke publik		✓			

3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				✓	
		2. Kerugian materi dengan nominal yang cukup besar			✓		
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan		✓			
		2. Terjadinya deface atau perubahan tampilan pada sistem		✓			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			✓		
		2. Pemerasan terhadap korban dengan ancaman				✓	
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual		✓			

b) Hasil Wawancara Nilai *Severity*

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada					✓
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting		✓			
		3. Malware dapat merusak jaringan komputer					✓

2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban				✓	
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				✓	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku			✓		
		4. Tabungan dikuras setelah masuk ke situs palsu					✓
		5. Mengambil data internal untuk dibocorkan ke publik			✓		
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				✓	
		2. Kerugian materi dengan nominal yang cukup besar					✓
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan			✓		
		2. Terjadinya deface atau perubahan tampilan pada sistem		✓			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress				✓	
		2. Pemerasan terhadap korban dengan ancaman					✓
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual			✓		

Lampiran 4 Hasil Wawancara Narasumber 3

PROFIL RESPONDEN

Nama : Letkol (E) Risman

Telepon :

Jabatan / Posisi : Kasi Analevsifor Satsiber Dispamsanal

a) Hasil Wawancara Nilai *Likehood*

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Likehood*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada			✓		
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting			✓		
		3. Malware dapat merusak jaringan komputer			✓		
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban			✓		
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				✓	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku		✓			
		4. Tabungan dikuras setelah masuk ke situs palsu			✓		
		5. Mengambil data internal untuk dibocorkan ke publik				✓	

3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin				✓	
		2. Kerugian materi dengan nominal yang cukup besar			✓		
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan		✓			
		2. Terjadinya deface atau perubahan tampilan pada sistem		✓			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			✓		
		2. Pemerasan terhadap korban dengan ancaman				✓	
		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual		✓			

b) Hasil Wawancara Nilai *Severity*

No	Potensi bahaya	Variabel Risiko Kecelakaan	*Severity*				
			Level 1	*Level 2*	*Level 3*	*Level 4*	*Level 5*
1	*Malware*	1. Malware dapat mencuri data-data perangkat dan informasi yang ada				✓	
		2. Terjadinya penyebaran virus untuk menghilangkan data-data penting	✓				

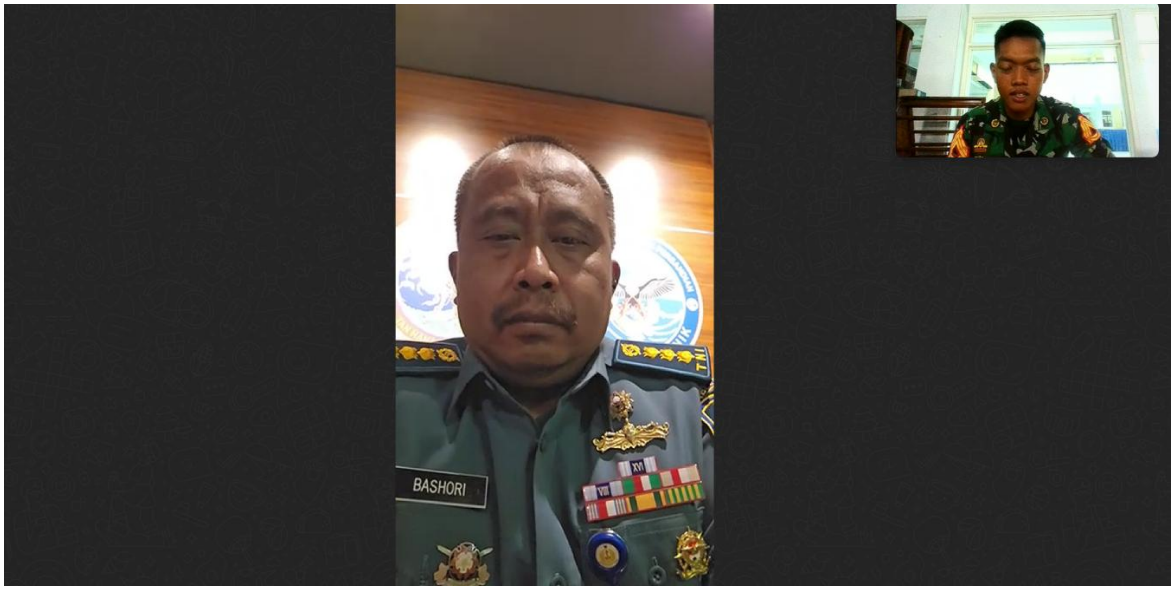
		3. Malware dapat merusak jaringan komputer			✓		
2	*Phising*	1. Data pribadi korban dicuri untuk disalahgunakan oleh pelaku atas nama korban					✓
		2. Pelaku mengambil data pribadi lalu digunakan untuk menyebarkan hoax				✓	
		3. Akun diretas lalu digunakan untuk mengirim pesan palsu oleh pelaku				✓	
		4. Tabungan dikuras setelah masuk ke situs palsu				✓	
		5. Mengambil data internal untuk dibocorkan ke publik		✓			
3	*Skimming*	1. Terjadinya pencurian informasi pribadi seperti username password dan pin					✓
		2. Kerugian materi dengan nominal yang cukup besar					✓
4	*Cracking*	1. Terjadinya kerusakan sistem karena terkena Cracking sehingga menghambat pekerjaan				✓	
		2. Terjadinya deface atau perubahan tampilan pada sistem		✓			
5	*Bullying*	1. Pelaku mengintimidasi korban hingga membuat stress			✓		
		2. Pemerasan terhadap korban dengan ancaman					✓

		3. Mencari foto yang tidak senonoh lalu digunakan sebagai bahan pelecehan seksual				✓	

Lampiran 5 Dokumentasi Pelaksanaan Wawancara

a) Narasumber 1: Laksamana Pertama Bambang Suseno Indro Pranoto S.H,CHRPM., M.Tr.Opsla

b) Narasumber 2: Kolonel Laut (E) Muhammad Bashori Alwi, S.T.,M.T.



c) Narasumber 3: Letkol (E) Risman