ISSN: 2477-5126
e-ISSN: 2548-9356

Penyesuaian Model Ketahanan Siber UMKM di Indonesia Dengan Nist Cybersecurity Framework

Sabri Balafif[1*)]
[1]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Dr Soetomo, Surabaya
[1]Jln. Semolowaru No.84, Menur Pumpungan, Kec. Sukolilo, Surabaya, Jawa Timur 60118, Indonesia
email: [1]sabri.balafif@gmail.com

***Abstract* — This research aims to evaluate the path to attaining Cyber Resilience in the digital transformation process of SMEs through the ability to mitigate and recover from attacks quickly while ensuring essential business operations continue based on the NIST framework, while the pilot model of cyber resilience refers to a series of initiatives for the adoption and utilization of IS / IT of the digital transformation strategy for SMEs that are vulnerable to various cyber attacks because SMEs are very limited in access to networking and resource development in building cyber resilience that ensures sustainability and improves business competitiveness. This research methodology is a qualitative descriptive analysis with Mapping from SWOT Analysis and assessing the feasibility of implementing initiatives based on the IT Balance Scorecard which is harmonized through the NIST framework. The results show that the implementation of initiatives that support the relationship between attack resistance and cyber resilience can be measured based on alertness to situations and expertise and proficiency in using technology to enforce resilience in cyberspace is conducted based on the NIST framework.**

Keywords* - *cyber resilience model, NIST Cybersecurity Framework , resistensi, SMEs

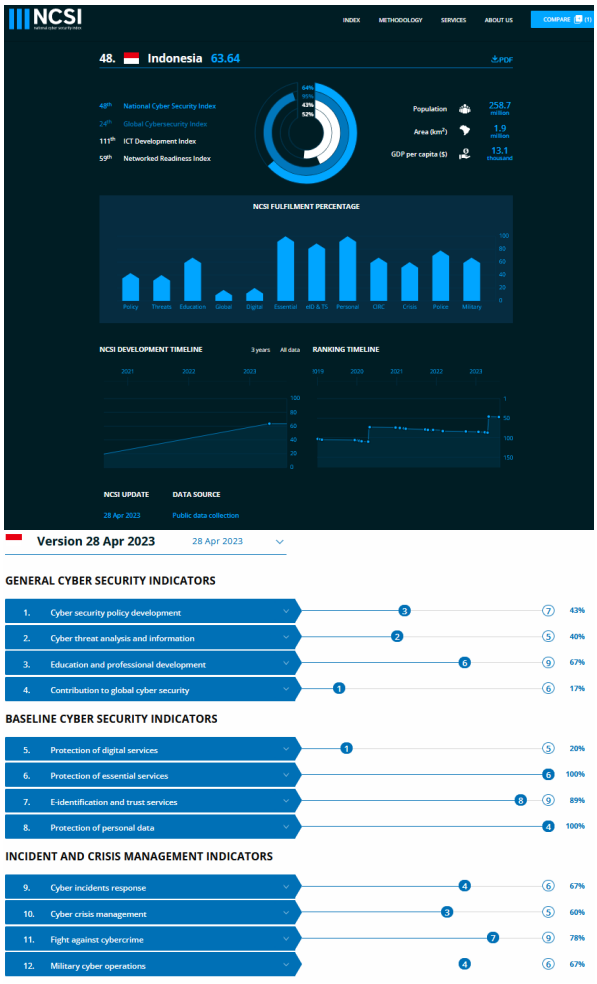
***Abstrak* – Penelitian ini bertujuan untuk menilai langkah mencapai Ketahanan Siber pada proses tranformasi digital UMKM melalui kemampuan untuk Memitigasi dan bangkit dari serangan dengan cepat seraya memastikan operasi bisnis yang esensial tetap berjalan berdasarkan kerangka kerja NIST, sedangkan contoh model ketahanan siber merujuk pada daftar inisiative adopsi dan utilisasi SI/TI dari strategi transformasi digital UMKM yang rentan terhadap berbagai serangan siber karena pelaku UMKM sangat terbatas dalam akses pengembangan networking dan sumberdaya dalam membangun ketahanan siber yang menjamin keberlanjutan dan meningkatkan daya saing usahanya. Metodologi penelitian ini bersifat analisis deskriptif kualitatif dengan Pemetaan dari Analisis SWOT dan penilian kelayakan implementasi inisiatif berdasarkan IT Balance Scorecard yang diselaraskan melalui kerangka kerja NIST. Hasil penelitian menunjukkan bahwa penerapan inisiatif yang medukung Hubungan Resistensi serangan dengan ketahan Siber dapat diukur berdasarkan kewaspadaan terhadap situasi serta keahlian dan kecakapan penggunaan teknologi untuk menegakkan ketahanannya di ruang siber melalui tiga aspek kerangka kerja NIST.**

***Kata Kunci* – Ketahanan siber , NIST Cybersecurity Framework, resistensi ,UMKM**

*) **penulis korespondensi**: Sabri Balafif
Email: sabri.balafif@gmail.com

I. PENDAHULUAN

Kasus peretasan sistem teknologi informasi (TI) dan pembobolan data yang menimpa sejumlah pelaku usaha dan instansi pemerintah marak terjadi. Terbaru, pembobolan 34 juta data pemegang paspor dan 337 juta data kependudukan di Indonesia. Merujuk pada laporan terbaru dari National Cyber Security Index (NCSI) tanggal 28 Apr 2023, tingkat keamanan siber Indonesia berada di peringkat 48 dengan poin 63,64, Ada 12 indikator yang digunakan NCSI dalam laporan tersebut, mulai dari perkembangan kebijakan keamanan siber, perlindungan data. pribadi, hingga peperangan melawan kejahatan siber.[1].



Gbr 1. National Cyber Security Index

UMKM Indonesia masih menjadi salah satu korban favorite para hacker dalam melakukan serangan, dikarenakan tingkat keamanan yang rendah, dapat dilihat dari Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20 tahun 2022 yaitu 38,96 poin dari 100 [1] serta salah satu negara strategis dalam perekonomian dunia. Walau UMKM sekarang ini telah mengakselerasikan cyber security dengan model ketahanan siber dalam transformasi digitalnya, seperti halnya perusahaan-perusahaan besar. Tetapi mereka belum menindaklanjutinya secara signifikan karena terkait kesadaran dan literasi yang cukup akan dampak kerugian alokasi biaya , waktu dan sumber daya manusia yang ditimbulkan jika tidak terus memperbaharui keamanan sibernya secara berkelanjutan, karena banyak UMKM berpikir bahwa keamanan siber terlalu mahal atau sulit, jika harus merujuk pada asas resistensi terhadap serangan dengan terus memperbaharui keamanan sibernya secara berkelanjutan. Walaupun faktanya, mereka mungkin akan mengalami kerugian yang lebih besar dari pada perusahaan yang lebih besar karena kejadian keamanan siber dapat merugikan dan mengancam kelangsungan bisnis mereka. Disisi lain, tuntutan tersebut tidak dapat dihindarkan karena tren perkembangan ancaman siber bersifat dinamis dan massif serta pregresif. Seperti contoh Serangan Distributed Denial of Service (DDoS) telah meningkat dalam beberapa tahun ini, dahulu DDoS hanya dirancang dan diluncurkan untuk merusak system melalui over flooding data, kini telah bertranfromasi dan terintegrasi dengan botnet untuk membentuk serangan canggih dan cenderung bertarget, dan tidak hanya digunakan untuk mengganggu layanan tetapi juga membuat sumber daya tertentu tidak dapat diakses atau pencurian uang [2] [3] [4].

Pada Dasarnya UMKM hanya pengguna dari layanan Perusahaan Software as a service (SaaS) seperti marketplace dan layanan berbasis online lain. Masalahnya menurut survei Accenture, hampir 80% organisasi memperkenalkan inovasi lebih cepat dari pada kemampuan mereka untuk melindunginya. Dukungan pemerintah dalam membangun *keamanan siber* dan *pertahanan siber* nasional secara organik melalui lembaga khusus yang memiliki otoritas penuh untuk mengelola dan menangani keamanan dunia maya yaitu Badan Siber dan Sandi Negara memang perlu pembenahan. Secara organik maksudnya keamanan dan pertahanan nasional dibangun oleh Penyelenggara Sistem Elektronik secara semesta dan berkesinambungan, hal tersebut dikarenakan pengimplementasian strategi yang telah dirancang untuk membangun cyber security yang ideal bagi Indonesia menjadi terhambat karena " (1) Aspek kelembagaan yang masih perlu dievaluasi dalam pencapaian sasaran strategis; (2) Aspek Ketatalaksanaan pedoman dan standar operasional; (3) prosedur yang belum diterapkan secara menyeluruh; (4) Aspek sumber daya manusia yang kualitasnya perlu ditingkatkan; (5) Aspek sarana dan prasarana yang terbatas serta system informasi yang belum terintegrasi sepenuhnya"[5].Peran pemerintah akan sangat dibutuhkan dalam kaitannya menghadirkan ketahanan dalam dunia siber (*Cyber Resilience*), dalam sektor industri khususnya menengah dan kecil seperti UMKM, karena ditingkat global, UKM berkontribusi terhadap lebih dari 90 persen ekonomi bisnis di seluruh dunia [6]. Namun, meskipun lembaga khusus telah dijalankan oleh pemerinta, pemerintah tidak bisa berdiri sendiri.

Pelaku usaha UMKM seharusnya tetap dapat menugaskan salah satu struktur atau lembaga dalam organisasinya untuk menjadi garda terdepan dalam keamanan transformasi digitalnya, karena ketahanan siber yang ideal dapat dibangun hanya dengan dukungan kesadaran keamanan siber yang memadai. Hal ini menunjukkan kepada kita bahwa implementasi keamanan dunia siber harus bersifat terpadu dan tidak hanya berpangku pada peran pemerintah dalam pertahanan dunia siber sangat terbatas untuk bertindak teknis pada seluruh aspek operasional personal pelaku usaha. Ketahanan siber diperlukan untuk memastikan bahwa operasional dapat terus berjalan secara berkesinambungan dan berlanjut, meskipun dalam kondisi diserang bahkan pasca serangan, keamanan siber itu sendiri merupakan aksi proaktif untuk melakukan mitigasi risiko agar dapat meminimalisir dampak yang dapat ditimbulkan.

NIST Cybersecurity Framework (NIST-CSF), merupakan best-practice untuk kerangka kerja ketahanan siber UMKM. Kerangka kerja tersebut dibagi menjadi lima bagian utama: identifikasi, proteksi, deteksi, respons, dan pemulihan. Jika dilihat secara keseluruhan, lima kata umum ini menawarkan perspektif holistik tentang rentang waktu mitigasi risiko kejahatan siber. Tugas-tugas yang dijelaskan di setiap fungsi dapat berfungsi sebagai peta jalan untuk operasional bisnis [7]. Penerapan keamanan siber UKM NIST memberikan metodologi kepada UMKM untuk mengidentifikasi dan mengelola risiko keamanan siber dengan menilai tingkat ancamannya. Bagi perusahaan kecil, mereka akan memiliki akses ke penilaian risiko bersifat swadaya dari NIST, sehingga mereka akan mengetahui di mana letak kerentanan dan memahami tindakan apa yang diperlukan untuk menetralisir potensi ancaman. Namun, standar yang tersedia masih sedikit dan biasanya difokuskan pada perusahaan besar yang memiliki proses bisnis yang terstruktur dengan baik [8]. Pada penelitian ini akan dilakukan penyesuaian agar standar tersebut dapat di terapkan oleh UMKM secara umum. Penyesuaian NIST Cybersecurity Framework sebagai kerangka kerja Ketahan Siber dilakukan dengan menyertakan aspek resistensi terhadap serangan siber dan ketahanan siber itu sendiri, guna bersama dan diterapkan untuk menjaga dan mempertahankan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi elektronik atau Sistem Elektronik., sehingga menyebabkan ekosistem relatif tidak terganggu ketika dihadapkan pada suatu gangguan, tetapi dalam kasus resistensi tidak ada reorganisasi internal (inisiatif dan adaptif) dan perubahan yang terjadi secara terus-menerus

II. PENELITIAN YANG TERKAIT

Dalam penelitian yang dilakukan oleh Ika Riswanti Putranti dkk dengan judul "Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah" disimpulkan bahwa "kompleksitas yang berkembang dari sistem dunia maya dan ancamannya memerlukan integrasi proses manajemen risiko dan proses manajemen ketahanan. Seringkali, ancamannya tidak diakui sampai terwujud dalam sistem siber dan karenanya mungkin terlewatkan dalam skenario ancaman yang diperiksa sebagai bagian dari penilaian risiko" [9]. Artinya jika dikaitan pada masalah yang dipaparkan pada penjelasan pembuka adalah "Penilaian Resiko berbasis kewaspadaan dan kesadaran" dapat menjadi solusi sebagai

ISSN: 2477-5126
e-ISSN: 2548-9356

pijakan dasar dalam merujuk prioritas perbaharuan yang dibutuhkan untuk keamanan digital yang di terapkan, agar biaya , waktu dan sumber daya yang dialokasikan dapat efektif dan efesien sehingga tidak lagi UMKM terjebak pada isu-isu inefisiensi dalam terus memperbaharui kemanan sibernya. Hasil dari penelitian tersbut juga setara dengan penelitian yang dilaksanakan oleh Bemenet Kasahun Gebremeskel dkk , yaitu bahwa bukan tugas yang mudah untuk mengurangi dan memahami serta mencegah adanya beragam serangan siber, namun ada pendekatan rasional untuk meminimalisir yaitu pertama, meningkatkan kesadaran akan keamanan siber melalui literasi berkelanjutan. Kedua yakni pembaruan metode dan pendekatan keamanan, khususnya yang berperan sebagai mitigasi dini guna memastikan bahwa semua system dan titik akhir telah diperbarui secara terstruktur, karena sebuah risiko penting yang harus diperiksa adalah risiko keamanan [10].

.

III. METODE PENELITIAN

Penelitian ini bersifat analisis deskriptif berbasis kualitatif, guna mengeksplorasi hasil secara intuitif dengan struktur sistematik. Sifat kualitatif yang dimaksudkan, adalah peneliti mencari interpretasi, pemahaman, definisi tentang suatu fenomena, kejadian melalui keterlibatan interaksi langsung maupun tidak langsung dalam obyek yang diteliti berdasarkan keilmuan yang membidanginya. Penelitian kualitatif merupakan metodologi ekplorasi yang memfokuskan hasil kajian berupa makna, definisi, konsep, karakteristik, dan pola termasuk deskripsi interpretasi dengan nalar saintifik mengenai fenomena tertentu secara spesifik yang memiliki sifat esensial dan komprehensif, kemudian disajikan secara naratif. Penelitian kualitatif melibatkan mekanisme ekplorasi dan akuisisi, termasuk analisis dan interpretasi secara kritis dan komprehensif untuk menghasilkan pemahaman mengenai permasalahan yang ekslusif serta sarat akan Pustaka emperis akan fenomena dan/atau obyek yang diteliti melalui tahapan (1) Pengumpulan Informasi : Mengidentifikasi susunan substansi dan ruang lingkup ; (2) Analisis Fungsionalitas: Menganalisis fungsi elemen-elemen yang telah diidentifikasi pada langkah sebelumnya dan mengevaluasi kebutuhan mereka terhadap tujuan penerapannya; (3) Spekulasi Inovatif: Mengembangkan solusi alternatif untuk memenuhi fungsionalitas yang diperlukan melalui Value Engineering berbasis brainstorming untuk menghasilkan solusi potensial perancangan dalam mencapai fungsionalitas yang diinginkan.
Penekanan dekskriptif penelitian ini untuk mempertegas, membuat fokus, dan mengatur data sedemikian rupa sehingga dapat menarik kesimpulan atau memperoleh pokok temuan, khususnya dalam mempertajam pemahaman hasil observasi keterkaitan fenomedan da/atau obyek tersebut pada suatu hal. Jenis data dalam penelitian ini bersumber dari data primer dan sekunder. Teknik pengumpulan data primer diperoleh dari studi literatur melalui buku dan artikel jurnal serta peraturan perundang-undangan yang terkait secara langsung pada keamanan siber. Di sisi lain, data sekunder dalam penelitian ini didapatkan melalui kajian interpretasi akan laporan berjangka dari Lembaga analisis penililaian akan perkembangan penerapan Langkah-langkah strategis untuk mencapai ketahanan siber secara dinamis.

Data Primer :

1. Kerangka kerja ketahanan siber UMKM NIST Cybersecurity Framework mencakup informasi tentang cara :
   a. Menyusun kebijakan dan protokol untuk melindungi;
   b. Membatasi akses karyawan ke data yang dilindungi;
   c. Mengenkripsi informasi yang keluar dan masuk;
   d. Menerapkan penyaring email dan internet
   e. Memperbaharui sistem operasi yang ada;
   f. Memberikan pelatihan kepada karyawan.

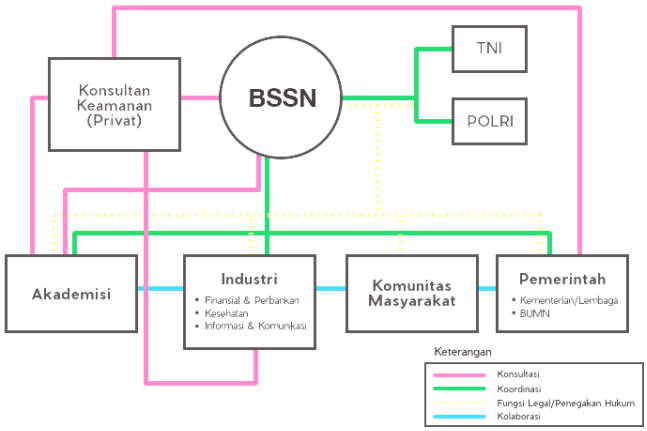
Adapun tahapannya adalah :

1. Identifikasi - Mendokumentasikan dan mengkategorikan
2. Melindungi - Mengembangkan perlindungan untuk semua layanan penting;
3. Mendeteksi - Identifikasi peristiwa ancaman keamanan
4. Merespon - Merencanakan respons secepat mungkin untuk menanggulangi serangan;
5. Memulihkan - Perencanaan jangka panjang untuk pemulihan aset yang hilang

seperti pada gambar 2 dibawah.

Gbr2. NIST Cybersecurity Framework (NIST-CSF)

2. REKOMENDASI RENCANA AKSI PADA STRATEGI KEAMANAN SIBER INDONESIA [11]



Gbr. 3 Rekomendasi Skema Koordinasi Multisektoral

Pada gambar 3 diatas , merupakan pola kuminkasi multi sectoral yang dibutuhkan untuk aksi yang meliputi tahap preventif, identifikasi, respons, dan pemulihan (recovery) atas serangan-serangan siber yang mengancam Indonesia. Selain identifikasi, tahap rencana aksi juga membatasi adanya tiga subjek yang menjadi fokus dalam implementasi strategi yang rekomendasikan yaitu (a) Kepentingan Pemerintah/Kedaulatan Negara (b) Infrastruktur Kritis dan (c) Masyarakat. Pembagian ini menggunakan pendekatan risk-based yang terbagi berdasarkan dampak yang akan ditimbulkan terhadap subjek yang berbeda.

Data Sekunder :

Kerangka kerja ketahanan siber UMKM Indonesia yang akan disusun merujuk pada aturan kerangka hukum cyber-security di Indonesia saat ini dibangun diantaranya berdasarkan atas dasar :

1. UU Informasi dan Transaksi Elektronik No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Dengan beberapa penyesuain sesuai **S**IARAN PERS NO. 17/HM/KOMINFO/02/2023 tentang Perubahan Kedua UU ITE untuk Harmonisasi dengan UU KUHP [12]. Dimana Menkominfo menyatakan UU ITE merujuk kepada Budapest Convention on Cybercrime serta memperbaharui ketentuan hukum pidana dengan memberikan konteks ruang siber pada ketentuan hukum pidana dan Menkominfo juga menyatakan sesuai pasal 622 ayat 1 huruf r UU KUHP terdapat ketentuan dalam UU ITE yang dicabut dan dinyatakan tidak berlaku, antara lain:
   a. Ketentuan pasal 27 ayat 1 mengenai kesusilaan dan ayat 3 mengenai penghinaan dan pencemaran nama baik;
   b. Ketentuan pasal 28 ayat 2 mengenai ujaran kebencian berdasarkan SARA;
   c. Ketentuan pasal 30 mengenai akses illegal;
   d. Ketentuan pasal 31 mengenai intersepsi atau penyadapan;
   e. Ketentuan pasal 36 mengenai pemberatan hukuman karena mengakibatkan kerugian terhadap orang lain;
   f. Ketentuan pasal 45 ayat 1 ancaman pidana terhadap pelanggaran pasal 27 ayat 1 terkait kesusilaan dan ayat 3 mengenai ancaman pidana terhadap pelanggaran pasal 27 ayat 3 terkait penghinaan dan pencemaran nama baik;
   g. Ketentuan pasal 45 ayat 2 mengenai ancaman pidana terhadap pelanggaran pasal 28 ayat 2 ujaran kebencian berdasarkan SARA;
   h. Ketentuan pasal 46 mengenai ancaman pidana terhadap pelanggaran pasal 30 terkait akses illegal;
   i. Ketentuan pasal 47 mengenai ancaman pidana terhadap pelanggaran pasal 31 terkait intersepsi atau penyadapan, dan;
   j. Ketentuan pasal 51 ayat 2 mengenai ancaman pidana terhadap pelanggaran pasal 36 terkait pemberatan hukuman karena mengakibatkan kerugian terhadap orang lain.
2. Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber .
3. Standar Nasional Indonesia (SNI) IEC/ISO 27001:2013 persyaratan untuk penetapan, penerapan, pemeliharaan, dan perbaikan berkelanjutan terhadap Sistem Manajemen Keamanan Informasi (SMKI) ;
4. SNI ISO/IEC 27018:2016, Teknologi informasi – Teknik keamanan - Petunjuk praktik perlindungan informasi personal (PII) dalam public cloud yang berperan sebagai pemroses PII ;
5. Indeks Keamanan Informasi (Indeks KAMI). Alat evaluasi untuk menganalisis kesiapan pengamanan informasi di instansi pemerintah berbasis ISO/IEC 27001:2009 (Dirjen Aplikasi Telematika, 2013).

IV. HASIL DAN PEMBAHASAN

Analisis faktor internal dan eksternal dalam SWOT Analisis dari sisi bisnis maupun sisi adopsi dan utilisasi SI/TI strategi transformasi digital UMKM . Dalam strategi kerangka kerja ketahan siber yang selaras dengan strategis bisnis UMKM diindonesia adalah sebagai berikut :

Faktor ***Strength*** **/ Kekuatan** Transformasi Digital UMKM indonesia :

1. Berfokus pada kepuasan dan kepercayaan pelanggan
2. Supply chain yang efektif (lead time < 3 hari)
3. marketplace di Indonesia bersifat incremental (senantiasa meningkat);
4. Harga Gaget seperti laptop dan Hp mulai terjangkau;
5. utilisasi e-commerce secara gratis melalui marketplace
6. online membuat Investasi Modal Usaha lebih terjangkau;
7. Keuntungan tambahan dari iklan, sponsor, dan promosi
8. Menjangkau Konsumen Lebih Luas;

Faktor ***Weakness*** / **Kelemahan** Transformasi Digital UMKM indonesia :

1. Kesadaran diri akan ketahanan siber;
2. Paradigma keamanan siber sebagai biaya bukan investasi;
3. Minimnya literasi dan pemanfaatan valuasi perusahaan berbasis factor Intangibe asset, seperti Goodwill.

Faktor ***Opportunities*** / **Peluang** Transformasi Digital UMKM indonesia :

1. Memiliki struktur tatakelola yang professional;
2. Mengurangi risiko human error dan kecurangan yang dilakukan internal
3. Penyeimbangan profitabilitas, efisiensi dan solvabilitas dengan pendekatan distruptif;
4. Tersedianya infrastruktur telekomunikasi baik berupa jaringan kabel dan nirkabel maupun satelit yang menjangkau seluruh wilayah UKM;
5. Adanya komunitas / SDM-Wira IT dan sarana pelatihan secara online dan gratis
6. Pergeseran perilaku masyarakat Indonesia dalam bertransaksi secara offline ke online.

Faktor ***Threats*** / **Ancaman** Transformasi Digital UMKM indonesia :

1. Serangan Hacker bisa terjadi kapan saja

2. Faktor Individu menjadi dominan
3. Penambahan Waktu Shifting Process;
4. Kompetitor bertambah banyak
5. Tren pasar muda berubah secara dinamis

Berdasarkan faktor diatas, penentuan bobot ditentukan lewat survey kuesioner yang diberikan kepada 3 orang pihak yang terkait penelitian ini. Orang tersebut adalah yaitu pelaku umkm, akademisi ICT dan praktisi ICT. Dimana pihak tersebut diminta untuk mengisi nilai dari rentang "1 sampai dengan 5". Jika semakin kecil nilainya berarti "tidak berarti penting" dan jika diisi nilai semakin besar berarti "sangat penting" bagi pihak yang diminta penilaian

Tabel 1. Hasil Survei Faktor Strategi Internal

Faktor Strategi Internal	**Survei Kuesioner**			**Survei Kuesioner**			**Bobot Rata-Rata**	**Rating**	**BxR**
S1	4	4	4	0,1026	0,1026	0,1053	0,1035	3	0,1035
S2	4	4	4	0,1026	0,1026	0,1053	0,1035	3	0,1035
S3	5	5	5	0,1282	0,1282	0,1316	0,1293	4	0,1293
S4	5	5	5	0,1282	0,1282	0,1316	0,1293	4	0,1293
S5	4	4	4	0,1026	0,1026	0,1053	0,1035	3	0,1035
S6	3	2	2	0,0769	0,0513	0,0526	0,0603	2	0,0603
S7	2	2	3	0,0513	0,0513	0,0789	0,0605	2	0,0605
S8	5	5	3	0,1282	0,1282	0,0789	0,1118	3	0,1118
Faktor ***Strength*** **/ Kekuatan**									**2,5427**
W1	5	5	5	0,1282	0,1282	0,1316	0,1293	3	0,42
W2	1	2	1	0,0256	0,0513	0,0263	0,0344	2	0,06
W3	1	1	2	0,0256	0,0256	0,0526	0,0346	4	0,12
Faktor ***Weakness*** / **Kelemahan**									**0,5954**
Koordinat X (Strength - Weakness)							1		**1,9474**

Penjelasan Nilai **0,1026** pada kolom survei 1 didapatkan dari perhitungan sebagai berikut:

$$= \frac{\text{Nilai Survei}_n}{\text{Total Survei}_n} \quad \frac{4}{39}$$

Tabel 2. Hasil Survei Faktor Strategi Eksternal

Faktor Strategi Eksternal	**Survei Kuesioner**			**Survei Kuesioner**			**Bobot Rata-Rata**	**Rating**	**BxR**
	1	**2**	**3**	**1**	**2**	**3**			
O1	5	5	5	0,1316	0,1316	0,1282	0,1305	4	0,5218
O2	1	1	1	0,0263	0,0263	0,0256	0,0261	3	0,0783
O3	4	4	4	0,1053	0,1053	0,1026	0,1044	3	0,3131
O4	4	4	4	0,1053	0,1053	0,1026	0,1044	3	0,3131
O5	4	4	4	0,1053	0,1053	0,1026	0,1044	3	0,4175
O6	4	4	4	0,1053	0,1053	0,1026	0,1044	4	0,4175
Faktor ***Opportunities*** / **Peluang**									**2,0612**
T1	5	5	5	0,1316	0,1316	0,1282	0,1305	3	0,3914
T2	4	4	4	0,1053	0,1053	0,1026	0,1044	4	0,4175
T3	4	4	4	0,1053	0,1053	0,1026	0,1044	4	0,4175
T4	2	2	3	0,0526	0,0526	0,0769	0,0607	3	0,1822
T5	1	1	1	0,0263	0,0263	0,0256	0,0261	2	0,0522
Faktor ***Threats*** / **Ancaman**									**1,4606**
Koordinat Y (Opportunities - Threats)							1		**0,6005**

Penjelasan Nilai **0,1316** pada kolom survei 1 didapatkan dari perhitungan sebagai berikut:

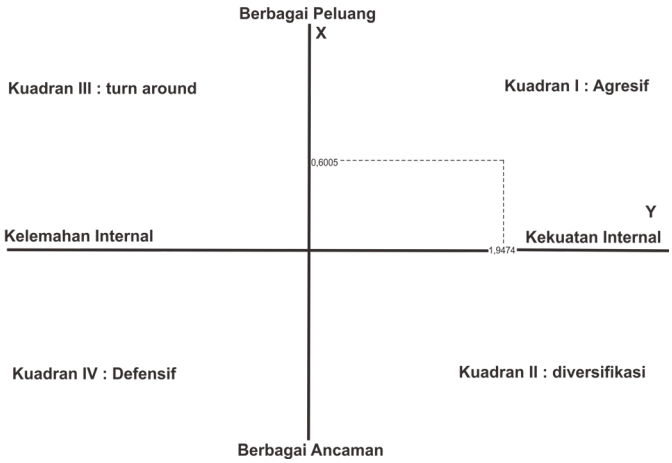
$$= \frac{\text{Nilai Survei}_n}{\text{Total Survei}_n} \quad \frac{5}{38}$$

Bobot adalah persentase pentingnya suatu indikator dalam sebuah umkm. Sedangkan "**rating**", adalah nilai kondisi berjalan dalam organisasi. Penentuan rating nilai 1 hingga 4 tersebut dinilai, berdasarkan subjektifitas terhadap

ISSN: 2477-5126
e-ISSN: 2548-9356

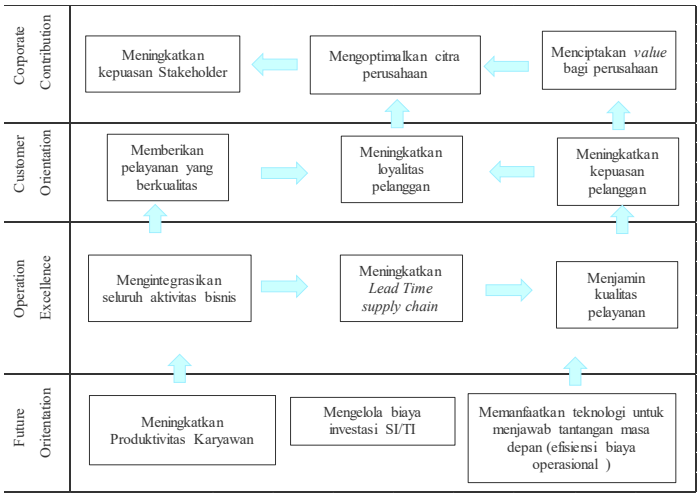
kondisi lingkungan UMKM yang bertranormasi dalam ekonomi digital saat melakukan observasi terhadap proses bisnis yang berjalan. Pemberian rating untuk fa faktor kekuatan (*strength*) bersifat "positif" diberi rating +4, sedangkan jika kekuatannya kecil diberi rating +1), Pemberian rating kelemahan (*weakness)* adalah kebalikannya, yaitu jika kelemahannya sangat besar bersifat "negatif" diberi rating 1 dan jika kelemahannya kecil ratingnya 4 [13].

ISSN: 2477-5126
e-ISSN: 2548-9356



Gbr. 4 Diagram SWOT tranformasi umkm indonesia

Terlihat pada Gambar 4 bahwa kondisi Tranformasi Digital UMKM indonesia berada pada koordinat (2, 0.625) maka kemudian strategi difokuskan pada strategi SO, yaitu strategi "Agresif" untuk menggunakan kekuatan internal UMKM untuk meraih peluang-peluang yang ada di lingkungan ekonomi digital. Langkah-langkah strategi **SO** tersaji pada Gambar 5 berdasarkan penilaian IT Balanced Scorecard.



Gbr 5. Strategy Map Tranformasi Digital UMKM

Alasan penggunaan kajian Strategy Map Tranformasi Digital UMKM menggunakan IT Balanced Scorecard untuk ekplorasi diluar ide-ide yang sudah jelas, seperti mengetahui bagaimana kinerja organisasi dan memahami arah yang akan dituju[14], seperti :

1. Mendukung argumen dengan beberapa data saat mempresentasikan solusi inisiatif;
2. Menyusun konteks bisnis dengan menyelaraskan inisiatif keamanan siber dengan bagian lain dari strategi;
3. Mengubah beberapa ide yang samar-samar seperti "lingkungan bisnis yang sangat aman yang memanfaatkan teknologi IT terbaru" menjadi sesuatu yang lebih nyata dengan indikator kinerja yang spesifik seperti pada table berikut :

Tabel 3. Perspektif *Corporate Contribution*

Objektif	Tolak Ukur
Meningkatkan kepuasan	• Peningkatan pendapatan • Menurunnya biaya operasional • Peningkatan loyalitas pelanggan
Mengoptimalkan citra perusahaan	
Menciptakan value	

Tabel 4 Perspektif *Customer Orientation*

Objektif	Tolak Ukur
Memberikan pelayanan yang berkualitas	*Delivery time* dari warehouse ke pelanggan
Meningkatkan loyalitas pelanggan	*Customer churn rate*
Meningkatkan kepuasan pelanggan	Ketersediaan merekomendasikan

Tabel 5 Perspektif *Operation Excellence*

Objektif	Tolak Ukur
Mengintegrasikan seluruh aktivitas bisnis	*Key Performance Indicator* baik secara individual, departemen dan organisasi
Meningkatkan *lead time supply chain*	Volume penjualan produk
Menjamin kualitas pelayanan	

Tabel 6 Perspektif *Future Excellence*

Objektif	Tolak Ukur
Meningkatkan produktivitas karyawan	*Key Performance Indicator*
Mengelola biaya investasi SI/TI	Rasio keuangan
efisiensi biaya operasional	Peningkatan profit dengan menurunnya biaya beban operasional

Pemetaan dari Analisis SWOT dan Fungsi NIST Freamwork dalam implementasi inisiatif tersaji dalam Tabel 3. Pemetaan dari Analisis SWOT dan Fungsi NIST Freamwork dalam implementasi inisiatif.

ISSN: 2477-5126
e-ISSN: 2548-9356

Table 3. Pemetaan dari Analisis SWOT dan Fungsi NIST Freamwork dalam implementasi inisiatif

Kode SWOT	No. inisiatif	Inisiatif Ketahanan siber berdasarkan rekomendasi Penelitan karya Yudhistira Nugraha dkk[15]	Indikator NIST Freamwork	Nilai	
				Saat ini [1]	Target
S,T	**9**	Mengembangkan promosikan yang lebih besar untuk meningkatkan kepercayaan dalam layanan online, seperti layanan e-government dan e-commerce.	**Identifikasi**		
			Business Environment	3	3
W,O	**3**	Membuat daftar proyek penting infrastruktur nasional dan membuka kerjasama dengan semua stake holder dan perusahaan yang bergerak dibidang proyek tersebut.	Asset Management	1	2
W,O	**1**	Mengembangkan strategi keamanan cyber nasional (NCSS).	Goverance	2	3
W,O	**10**	Mengembangkan strategi pemasaran standar untuk mempromosikan privasi online untuk melindungi data pribadi.	Risk Assessment	2	3
S,T	**7**	Mengembangkan strategi komunikasi cybersecurity untuk memperkuat dan memperluas kampanye cybersecurity nasional.	Risk Management Strategy	2	2
			Protect		
			Access Control	3	3
W,O	**4**	Mengadakan pelatihan manajemen krisis tingkat nasional dengan melibatkan semua yang berkepentingan dalam rangka persiapan yang kuat dan matang dalam penanganan insiden siber.	Awerness/Training	2	2
W,O	**5**	Membuat dan membangun masyarakat yang peka dan peningkatan kemampuan militer untuk melindungi kepentingan nasional di dunia maya.			
W,O	**12**	Mengadakan program pendidikan dan pelatihan keamanan siber pada setiap karyawan pemerintah, BUMN dan swasta.			
S,T	**2**	Memperkuat peran dan koordinasi fungsi ID-SIRTII / CC sebagai nasional CERT.	Data Security	2	3
S,T	**13**	Membuat registrasi nasional untuk jaminan informasi dan dewan pakar keamanan siber lintas sektor (publik dan privat) untuk menumbuhkan bakat baru sebagai sebuah profesi.	Protective Process dan Procedures	2	3
S,T	**20**	Memberikan subisidi terhadap perusahaan dalam negeri yang memberikan kontribusi produk dalam masalah kemanan siber dan mendorong pangsa pasarnya.	Maintenance	2	3
			Protective Technologies	2	3
S,T	**8**	Pengembangan portal nasional yang memegang kendali penuh tentang kewaspadaan tentang siber baik di tengah masyarakat, pemerintah, dan swasta.	**Detect**		
			Anomalies/Event	3	3
S,T	**11**	Mengidentifikasi pusat keunggulan pendidikan dan penelitian tentang keamanan siber untuk menemukan kekuatan dan memberikan investasi terfokus untuk mengatasi kesenjangan yang ada.	Security Continuos Monitoring	3	3
S,T	**19**	Membuat unit kerja pemerintah di bawah kementrian terkait yang memantau dan mengendalikan langsung dalam hal keamanan dan ketahanan siber Indonesia.	Detections Process	2	2
S,T	**6**	Membangun tim respon darurat dalam mengantisipasi segala kemungkinan buruk yang mungkin terjadi.	**Respond**		
			Respond Planning	2	2
S,T	**17**	Membuat sistem pelaporan tunggal operator sistem elektronik untuk pelayanan publik untuk melaporkan dan mengungkapkan insiden siber dan pencurian data sehingga dapat dilakukan aksi/ tindakan.	Communication	3	3
			Analysis	2	3
W,O	**16**	Ketegasan dalam penegakkan hukum dan peningkatan kemampuan jaksa dalam penyelidikan kejahatan siber dan membawa nya ke pengadilan.	Mitigations	3	3
W,O	**15**	Meninjau ulang segala aturan hukum yang ada, sebagai contoh perubahan UU ITE tentang pasal yang ada dalam undang-undang tersebut apakah masih relevan atau tidak dalam memerangi kejahatan siber	Improvement	1	3
			Recover		
			Recovery Planning	2	2
S,T	**14**	Meningkatkan kewaspadaan oleh pejabat pemerintah dan seluruh perusahaan yang memegang peranan penting tentang kemanan data sensitive tentang bahaya nya interaksi siber.	Improvements	1	3
S,T	**18**	Menghimbau peningkatan kemanan dalam proses pengadaan barang jasa pemerintah dalam rangka penguatan sistem keamanan siber nasional.	Communications	1	3

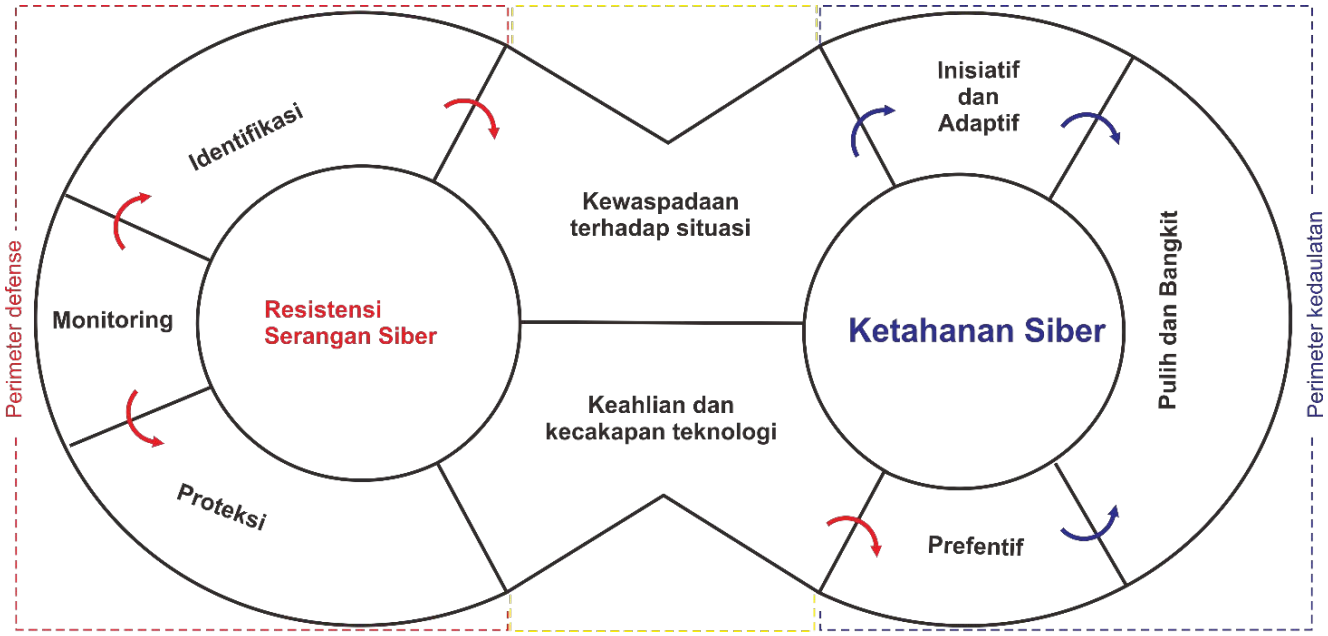
ISSN: 2477-5126
e-ISSN: 2548-9356

Ketahanan Siber adalah persiapan organisasi untuk menghadapi gangguan aktivitas bisnis yang disebabkan oleh serangan tersebut, kemampuannya untuk bangkit dari kekacauan, dan kemampuan sistemik untuk beradaptasi dan berkembang dari setiap serangan. Hal ini mengharuskan organisasi untuk memahami lingkungan operasi internal dan ekosistem digital mereka. Pendekatan dan model ketahanan siber yang dirangkum merupakan kerangka kerja ketahanan siber manajerial karena fokusnya pada praktik manajerial. Selain itu, kerangka kerja ini mengingat konsep-konsep Meninjau kemampuan digitalisasi berdasarkan pengaruh teknologi digital terhadap akselerasi proses bisnis seperti : Penggunaan sumber daya yang heterogen [16]; Kecakapan improvisasi [17] [18]; Memiliki akase informasi dan pengetahuan secara online [19]; Meningkatkan keterampilan belajar secara terus-menerus guna evaluasi kemajuan lingkungan digital dan penyesuaian kembali sumber daya secara efisien dengan perencanaan dan persiapan melalui kompetensi, adaptasi terhadap konteks, dan belajar dari pengalaman, yang merupakan ciri khas kemampuan digitalisasi [10] .

Untuk mencapai Ketahanan Siber, perusahaan juga harus mengembangkan kemampuan untuk Memitigasi dan bangkit dari serangan dengan cepat seraya memastikan operasi bisnis yang esensial tetap berjalan, meskipun dalam kondisi terdegradasi atau menggunakan sarana alternatif atau disebut juga memiliki Resistensi. Secara garis besar disimpulkan bahwa baik resistensi maupun resiliensi adalah kedua Langkah yang terangkai. 8 tugas yang terlibat dalam penyesuai kerja tersebut berdasarkan pada hubungan Resistensi serangan dengan ketahan Siber :

1. Mengidentifikasi alasan untuk melakukan penilaian. Nyatakan dengan jelas tujuan dan alasan penilaian kepada semua karyawan dan memperjelas ruang lingkup penilaian. harus mencakup area di mana data yang dilindungi dibuat, dikirim, dan disimpan;
2. Identifikasi jenis ancaman. Tentukan jenis ancaman yang dihadapi, atau peristiwa seperti pemadaman listrik atau phishing;
3. Identifikasi kerentanan. menemukan kerentanan dalam sistem, jaringan, atau penerapan yang dapat membahayakan data;
4. Tentukan seberapa besar kemungkinan terjadinya pelanggaran. Dengan menggunakan tahapan yang berbeda pada panduan penilaian risiko, tentukan kemungkinan terjadinya pelanggaran data;
5. Tentukan dampak dari pelanggaran tersebut. Setelah Anda mengetahui kemungkinan terjadinya pelanggaran, Anda dapat menentukan dampak negatif yang akan ditimbulkan terhadap Perusahaan;
6. Penentuan risiko. Menggabungkan kemungkinan dan dampak ancaman akan memberi Anda gambaran tentang penentuan risiko bisnis;
7. Hasil evaluasi. Karyawan dan manajemen harus mengetahui hasil penilaian risiko sehingga mereka dapat mulai menerapkan praktik dan kebijakan yang direkomendasikan;
8. Pertahankan rekomendasi penilaian. Setelah rekomendasi diterapkan, UKM harus mengambil langkah yang tepat untuk memastikan risiko telah ditanggulangi.

Kedelapan tugas tersebut secara konsuptual tersusun dalam pola hubungan kritis seperti pada gambar 3 dibawah.



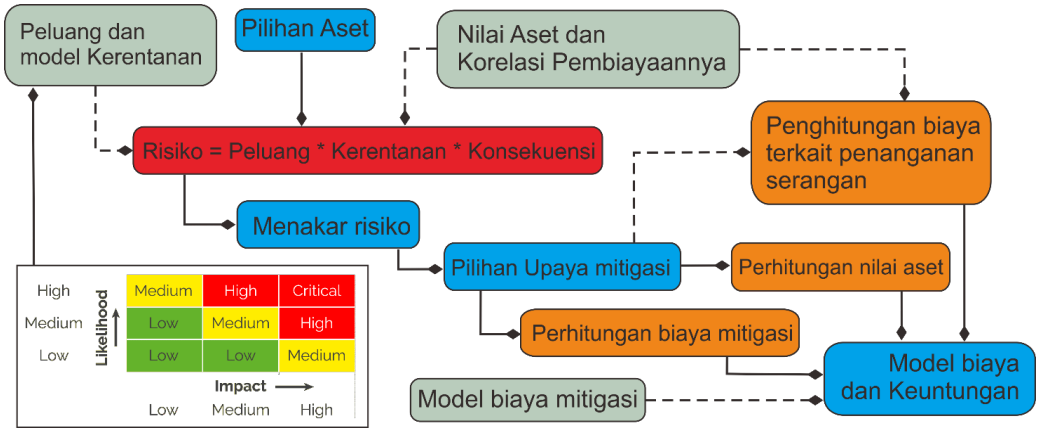
Gbr 6. Hubungan Resistensi serangan dengan ketahan Siber

ISSN: 2477-5126
e-ISSN: 2548-9356

Pada gambar hubungan resistensi serangan dengan ketahan Siber diatas merupakan harmonisasi keteraturan hubungan yang terjalin berdasarkan kebutuhan ketahanan siber yang mensyaratkan bahwa, meskipun perusahaan berupaya untuk mengantisipasi insiden, mereka juga harus memahami situasi operasional internalnya dan ekosistem digitalnya dengan cukup matang untuk mengembangkan dan melaksanakan rangkaian proses mempercepat deteksi keberhasilan penyerangan dan mengatasi dan merespons serangan yang teridentifikasi. Perimeter defense sebagai media yang menjadi komponen pertahanan standar dan panduan dalam menjalankan proses pengamanan. Lima area fokus untuk lima langkah menuju ketahanan siber untuk UKM dan pasar menengah adalah (1) Identifikasi - Pahami lingkungan dan risiko siber secara keseluruhan; (2) Melindungi - Menerapkan perlindungan yang tepat untuk mengatasi peristiwa keamanan siber; (3) Mendeteksi - Menjaga visibilitas ke dalam jaringan sehingga dapat mendeteksi intrusi; (4) Merespon dengan kewaspadaan dan pengembangan kemampuan dan teknologi - Mengasumsikan pelanggaran akan terjadi dan memiliki rencana yang tepat; (5) Memulihkan - akses untuk pemulihan secara efektif [20]. Strategi keamanan siber difokuskan pada perlawanan terhadap serangan siber yang mengarah pada penerapan kontrol dalam upaya untuk melindungi organisasi, seiring dengan semakin matangnya regulasi dan kerangka kerja keamanan siber, organisasi beserta praktik-praktik yang matang mulai menerapkan Arsitektur Zero Trust, yaitu strategi tingkat tinggi yang mengasumsikan bahwa individu dan perangkat serta layanan yang mencoba terhubung dan/atau mengakses sumber daya perusahaan, bahkan yang ada di dalam jaringan sekalipun, tidak dapat dipercaya begitu saja, untuk menyadari bahwa hal yang tidak dapat dihindarkan lebih mungkin terjadi dari pada dicegah, sehingga mengubah dari resistensi menuju resiliensi. mitigasi dapat ditentukan berdasarkan penilaian dampak dari resiko. Pada gambar 4 , terdapat 4 tingkat resiko yang dimaksud mengadopsi ISO Standard No. 31000:2018 [21] , yaitu :

1. Status risiko “High/Tinggi” menunjukkan bahwa sebuah sistem memiliki risiko yang parah dan langsung mengalami peristiwa yang merusak. Peristiwa ini termasuk serangan siber atau kegagalan peralatan yang akan mengakibatkan penghentian yang menyeluruh, peretasan informasi yang masif, atau terhentinya operasional sistem jika dibiarkan tanpa penanganan;
2. Risiko keamanan siber “**Medium/sedang”** berarti ada kemungkinan aktivitas anomaly .Tingkat potensi kerusakannya sedang tidak langsung merusak, peristiwa berisiko sedang dapat berkembang menjadi risiko serius jika tidak segera ditindaklanjuti;
3. Risiko keamanan siber yang “**Low/rendah”** berarti hanya ada sebagian kecil anomali di luar kekhawatiran yang biasa terjadi pada peristiwa kejahatan siber. Pada status risiko rendah, aktivitas jaringan masih berjalan normal. Pada status risiko rendah, aktivitas jaringan dianggap normal.Tidak ada peristiwa besar atau berbahaya yang terjadi di sistem Anda. Namun, penting untuk dicatat bahwa status tanpa ancaman bukan berarti tidak ada risiko sama sekali. Jika sistem terkoneksi ke jalur internet, selalu ada risiko serangan siber.

Mengapa Aset yang menjadi objek utama dan bukan data? Yang pertama dan terutama, pelanggan mengandalkan perusahaan untuk memberikan layanan dan produk yang mereka butuhkan, dan Aset ICT adalah perangkat operasional yang menjalankan proses tersebut. Serangan siber tidak hanya berimplikasi pada data pelanggan, tetapi yang lebih penting lagi, mengganggu penyampaian layanan. Oleh karena itu, gangguan layanan yang berkepanjangan akan jauh lebih merusak. pelanggan daripada pelanggaran data saja. Sangat mudah untuk melihat bagaimana prioritas itu bekerja. Tanyakan pada diri sendiri: Apakah lebih memilih rumah sakit yang dapat menjalankan operasionalnya untuk merawat kita, selama keadaan darurat medis, atau rumah sakit yang mengalami kegagalan system ?.



Gbr 7. **Penilaian dampak resiko (Frumento & Dambra, 2018) dengan penyesuaian peneliti**

V. KESIMPULAN

Secara garis besar, penyesuain kerangka kerja NIST Cybersecurity Framework adalah untuk mempertegas langkah pelaksanaan dalam hubungan Resistensi serangan dengan capaian ketahan Siber yang akan diharapkan. Pengasan tersebut diwujudkan dengan menjadikan aspek kewaspadaan terhadap situasi dan Pengembangan Keahlian dan kecakapan akan teknologi sebagai jembatan penghubung capaian ketahan Siber berdasarkan kemampuan resistensi serangan yang dimiliki oleh organisasi, karena fokus ketahan siber haruslah pada respons dan resistensinya, bukan pencegahan menyeluruh. Kejadian serangan siber kini semakin mungkin terjadi di lingkungan bisnis digital seperti Serangan malware menyebabkan bisnis kehilangan cukup besar dalam bentuk hilangnya pendapatan, penghentian operasional, dan kerusakan reputasi. Cara terbaik untuk menangani insiden dan pelanggaran keamanan yang tak terelakkan adalah dengan membuat jaringan dan bisnis tangguh dengan kewaspadaan dan kecakapan dalam pengembangan penerapan teknologi tepat guna.

UCAPAN TERIMA KASIH

Segala puji dan syukur penulis panjatkan kehadirat Tuhan Yang Maha Esa. Karena berkat, rahmat dan karunia serta mukzizat-Nya, sehingga penulis dapat menyelesaikan.

DAFTAR PUSTAKA

[1] National Cyber Security Index, "Skor Indeks Keamanan Siber," 2023. [Online]. Available: https://ncsi.ega.ee/country/id/

[2] O. Yoachimik and J. Pacheco, "DDoS threat report for 2023 Q2," 2023. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2023-q2/

[3] National Vulnerability Database, "CVE-2022-26143," 2022. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-26143

[4] W. Guo, H. Qiu, Z. Liu, J. Zhu, and Q. Wang, "The Evaluation of DDoS Attack Effect Based on Neural Network," *Secur. Commun. Networks*, vol. 2022, p. 5166323, 2022, doi: 10.1155/2022/5166323.

[5] Y. Ginanjar, "Strategi Indonesia Membentuk Cyber Security Dalam Menghadapi Ancaman Cyber Crime Melalui Badan Siber Dan Sandi Negara," *J. Din. Glob.*, vol. 7, no. 02, pp. 291–312, 2022, doi: 10.36859/jdg.v7i02.1187.

[6] World Bank Group, "Improving SMEs' access to finance and finding innovative solutions to unlock sources of capital.," 2023. https://www.worldbank.org/en/topic/smefinance (accessed Jul. 27, 2023).

[7] NIST, "THE NIST CYBERSECURITY You may have heard about the," *Cyber Secur. Polit.*, pp. 1–4, 2020.

[8] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *J. Cybersecurity Priv.*, vol. 1, no. 2, pp. 219–238, 2021, doi: 10.3390/jcp1020012.

[9] I. R. Putranti, A. Amaliyah, and R. Windiani, "Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah," *J. Ketahanan Nas.*, vol. 26, no. 3, p. 359, 2020, doi: 10.22146/jkn.57322.

[10] B. K. Gebremeskel, G. M. Jonathan, and S. D. Yalew, "Information Security Challenges During Digital Transformation," *Procedia Comput. Sci.*, vol. 219, pp. 44–51, 2023, doi: 10.1016/j.procs.2023.01.262.

[11] A. Rahmadiani, A. P. K. Mantovani, S. U. Hariz, J. Haryanto, and F. F. Aidad, "Strategi Keamanan Siber Indonesia Rekomendasi Rencana Aksi Dan Implementasi," *Cent. Digit. Soc.*, vol. 1, no. 69, pp. 5–24, 2019.

[12] kominfo, "SIARAN PERS NO. 17/HM/KOMINFO/02/2023," Jakarta, Feb. 2023. [Online]. Available: https://www.kominfo.go.id/content/detail/47389/siaran-pers-no-17hmkominfo022023-tentang-menkominfo-perubahan-kedua-uu-ite-perlu-harmonisasi-dengan-uu-kuhp/0/siaran_pers

[13] D. Leigh, "SWOT Analysis," in *Handbook of Improving Performance in the Workplace*, vol. 2, John Wiley & Sons, Ltd, 2010, pp. 115–140. doi: 10.1002/9780470587102.ch5.

[14] T. Herath, H. Herath, and W. G. Bremser, "Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management," *Inf. Syst. Manag.*, vol. 27, no. 1, pp. 72–81, Jan. 2010, doi: 10.1080/10580530903455247.

[15] Y. Nugraha, "The future of cyber security capacity in Indonesia," 2016.

[16] A. Mishra, P. Konana, and A. Barua, "Antecedents and Consequences of Internet Use in Procurement: An Empirical Investigation of U.S. Manufacturing Firms," *Inf. Syst. Res.*, vol. 18, pp. 103–120, 2007, doi: 10.1287/isre.1070.0115.

[17] P. Pavlou and O. Sawy, "The 'Third Hand': IT-Enabled Competitive Advantage in Turbulence Through Improvisational Capabilities," *Inf. Syst. Res.*, vol. 21, pp. 443–471, 2010, doi: 10.1287/isre.1100.0280.

[18] O. Sawy, A. Malhotra, Y. Park, and P. Pavlou, "Seeking the Configurations of Digital Ecodynamics: It Takes Three to Tango," *Inf. Syst. Res.*, vol. 21, pp. 835–848, 2010, doi: 10.1287/isre.1100.0326.

[19] A. Rai, R. Patnayakuni, N. Seth, and N. Patnayakuni, "Firm Performance Impacts of Digitally Enabled Supply Chain Integration Capabilities," *MIS Q.*, vol. 30, pp. 225–246, 2006, doi: 10.2307/25148729.

[20] R. Kissel, "Small Business Information Security : The Fundamentals Small Business Information Security : The Fundamentals," *Natl. Inst. Stand. Technol. Interag. Rep.*, vol. 7621, p. 20, 2016, doi: 10.6028/NIST.IR.7621r1.

[21] International Organization for Standardization, "ISO Standard No. 31000:2018 . Risk management. Guidelines," 2018