Studi Literatur: Analisis Persepsi UMKM di Indonesia Terhadap *Cyber Security* Menggunakan Model *Protection Motivation Theory* (PMT)

Septian Reri Winarto[1], Rahadian Bisma[2]

[1,2] Sistem Informasi, Teknik Informatika, Universitas Negeri Surabaya
[1]septian.17051214046@mhs.unesa.ac.id
[2]rahadianbisma@unesa.ac.id

***Abstrak*— Perkembangan teknologi pada era sekarang ini telah mengambil andil dalam bermacam aspek kehidupan manusia, salah satunya adalah bidang ekonomi. Namun, tak sedikit pelaku bisnis atau ekonomi yang belum memanfaatkan teknologi untuk mendukung operasional bisnis mereka. Pelaku ekonomi yang salah satunya memegang andil dalam kemajuan ekonomi di Indonesia yaitu Usaha Mikro, Kecil, dan Menengah (UMKM). Besarnya jumlah UMKM di Indonesia tidak sebanding dengan pemanfaatan teknologi yang telah dilakukan. Bahkan, data menunjukkan angka yang sangat kecil terkait pemanfaatan teknologi oleh UMKM di Indonesia. Oleh sebab itu, penelitian ini memiliki tujuan untuk memahami bagaimanakah persepsi UMKM di Indonesia terkait intensinya mengadopsi teknologi yang ditinjau dari sudut pandang *Cyber Security*. Model yang diadopsi dalam penelitian ini adalah *Protection Motivation Theory* (PMT). Penelitian ini dilakukan dengan mencari referensi-referensi dari literatur yang relevan dengan topik dan konteks penelitian, lalu melakukan perbandingan dengan kondisi UMKM di Indonesia. Faktor-faktor yang muncul dari hasil penelitian terdahulu ditelaah dan dianalisa dengan kondisi UMKM di Indonesia. Faktor-faktor yang diasumsikan dapat memberikan pengaruh kepada UMKM di Indonesia dalam mengadopsi teknologi dari sudut pandang *Cyber Security*, antara lain *Perceived Severity*, *Perceived Vulnerability*, *Response Efficacy*, *Self-Efficacy*, dan *Response Cost*, serta dilakukan penambahan variabel *Habit* dengan asumsi bahwa intensi dapat juga dipengaruhi oleh kebiasaan.**

***Kata Kunci*— Keamanan Siber, Kejahatan Siber, *Protection Motivation Theory*, Kebiasaan, UMKM**

I. PENDAHULUAN

Teknologi menjadi satu diantara berbagai aspek yang sedang dijadikan sebagai tolak ukur perkembangan kehidupan manusia modern. Pengembang teknologi sedang berlomba-lomba untuk dapat menciptakan sebuah teknologi, sehingga perkembangan teknologi saat ini memiliki tren yang sangat berubah-ubah dan semakin canggih. Apa yang menjadi tren teknologi saat ini, bisa jadi akan berubah menjadi tren teknologi baru keesokan harinya. Oleh karena hal tersebut, masyarakat dituntut untuk dapat beradaptasi dengan teknologi, dengan cara mengimplementasikan dan memanfaatkan teknologi yang ada pada aktivitas atau kegiatan sehari-hari. Pemanfaatan teknologi pada kehidupan masyarakat dapat dilihat dengan adanya sistem pembayaran pajak berbasis digital (*online*), sistem pendidikan jarak jauh dalam jaringan, dan sistem antrian *online*.

Selain dalam kehidupan sehari-hari, pemanfaatan internet juga dapat dilakukan oleh pelaku ekonomi dalam mendukung operasional bisnis mereka. Salah satu pemanfaatan teknologi oleh pelaku bisnis adalah memanfaatkan internet sebagai media promosi untuk memasarkan produk atau jasa mereka [1]. Salah satu pelaku ekonomi yang memegang tanggungjawab substansial bagi perekonomian Indonesia adalah Usaha Mikro, Kecil, dan Menengah (UMKM). Usaha Mikro, Kecil, dan Menengah (UMKM) menjadi salah satu sektor penyumbang perekonomian terbesar sekaligus memegang peran penting dalam mengamankan jaring pertumbuhan perekonomian di dunia, terlebih lagi dalam keadaan krisis.

Oleh karena besarnya kontribusi yang diberikan, UMKM menjadi salah satu pelaku ekonomi yang mengambil perhatian yang besar terhadap perkembangannya, salah satunya adalah dalam pemanfaatan teknologi. Merujuk dari hasil riset Mckinsey Institute, bahwa pada tahun 2017, dari total 59,9 juta unit UMKM di Indonesia, hanya ada sekitar 3,97 juta unit UMKM yang sudah memanfaatkan teknologi. Data tersebut menunjukkan angka yang sangat kecil, yaitu hanya sekitar 7% UMKM di Indonesia yang telah melek teknologi, hal ini mengindikasikan bahwa kemampuan UMKM dalam beradaptasi dengan teknologi sangat lambat.

Pemanfaatan teknologi oleh UMKM dapat dilakukan dengan bermacam cara, salah satunya yaitu dengan mengadopsi *e-commerce*. *E-commerce* (*Electronic Commerce*) adalah sebuah *platform* yang didalamnya terdapat proses penjualan dan pembelian barang, jasa, dan/atau informasi melalui media jaringan komputer yaitu internet [2]. Terlebih lagi, Indonesia merupakan pasar potensial *e-commerce*, sebesar 77% dari pengguna internet di Indonesia, memanfaatkan internet untuk mencari informasi terkait produk yang dicari, sekaligus berbelanja secara *online*, selain itu jumlah pelanggan *online shop* di Indonesia juga mencapai 8,7 juta orang [2].

Namun, potensi tersebut belum sepenuhnya dilihat oleh UMKM sebagai peluang yang menjanjikan. Padahal, pemanfaatan teknologi oleh pelaku bisnis terbukti dapat menaikkan omzet, aset, dan jangkauan pemasaran hingga 30% [1].

Teknologi memang memberikan manfaat, namun masyarakat khususnya UMKM perlu mengetahui hal-hal krusial yang harus diperhatikan ketika memanfaatkan teknologi. Perlu diketahui bahwa pemanfaatan teknologi juga

membawa risiko yang mungkin dapat mengancam keberlangsungan usaha pelaku bisnis. Risiko yang dapat membahayakan pelaku usaha dalam memanfaatkan teknologi, yaitu adanya ancaman dari *attacker*, *spammer*, maupun kejahatan kriminal siber lainnya, yang bahkan meningkat secara signifikan pada akhir-akhir ini. Kejahatan siber (*Cyber crime*) dapat membawa dampak buruk bagi organisasi publik maupun swasta, seperti menyebabkan kerugian finansial yang tidak sedikit, tidak berfungsinya sistem komputer, dan perusakan informasi penting, serta dapat membahayakan *integrity* dan *confidentiality* dari suatu jaringan [3]. Oleh sebab itu, pemanfaatan teknologi harus didasari oleh kesadaran terhadap kejahatan siber (*cyber crime awareness*) yang mengintai dan dapat terjadi sewaktu-waktu. Salah satunya yaitu dengan memberikan perhatian lebih terhadap *cyber security* organisasi, yang dapat dilakukan dengan cara mengelola risiko dari ancaman *cyber crime*.

Oleh sebab itu, diperlukan telaah literatur untuk mengasumsikan terkait indikator apa saja yang sekiranya dapat berdampak pada intensi UMKM di Indonesia dalam mengadopsi teknologi, namun dilihat dari aspek keamanan siber (*cyber security*). Analisis persepsi dilakukan dengan menggunakan model *Protection Motivation Theory* (PMT), yang merupakan sebuah konsep dalam menggambarkan intensi atau minat mengadopsi teknologi yang dilihat dari aspek ancaman maupun tanggapan atas kejahatan siber (*cyber crime*). Hasil dari kajian literatur ini diharapkan dapat menjadi *information knowledge* bagi UMKM di Indonesia agar *aware* terhadap *cyber crime* dan dapat mengambil langkah yang tepat dalam melakukan perencanaan *cyber security* maupun mitigasi risiko.

II. PEMBAHASAN

Literatur yang dipilih adalah yang sesuai dan relevan dengan topik pada penelitian ini dan siap untuk dilakukan telaah, diantaranya terdapat pada tabel dibawah ini:

TABEL I
DAFTAR LITERATUR TERDAHULU

No.	Judul Artikel Ilmiah	Penulis	Tahun
1.	The Influence of Hardiness and Habit on Security Behaviour Intention	Queen A. Aigbefo, Yvette Blount, dan Mauricio Marrone	2020
2.	Understanding Users Information Security Awareness and Intentions: A Full Nomology of Protection Motivation Theory	Farkhondeh Hassandoust dan Angsana A. Techatassanasoontorn	2020
3.	Pentingnya Sistem Informasi Akuntansi yang Handal Terhadap Bencana Pada Sektor Pemerintahan	Fifi Yusmita dan Evayani	2020
4.	Analisis Faktor-faktor yang Mempengaruhi Perilaku Pengguna Sistem Informasi Akademik Mahasiswa dalam Penciptaan Kata Sandi Kuat dengan Menggunakan Protection Motivation Theory (Studi pada XYZ)	Yustiyana April Lia Sari, Ari Kusyanti, dan Retno Indah Rokhmawati	2018
5.	Understanding Smartphone Security Behaviors: An Extension of The Protection Motivation Theory with Anticipated Regret	Silas Formunyuy Verkijika	2018
6.	Costly but Effective: Comparing The Factors That Influence Employee Anti-Malware Behaviours	John M. Blythe dan Lynne Coventry	2018
7.	Adopting Sustainable Behavior in Institutions of Higher Education: A Study on Intentions of Decision Makers in The MENA Region	Dr. Sultan O. Almarshad	2017
8.	Comparing Three Models to Explain Precautionary Online Behavioural Intentions	Jurjen Jansen dan Paul van Schaik	2017
9.	Gender Difference and Employees' Cybersecurity Behaviors	Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, dan Li Xu	2017
10.	"Security Begins at Home": Determinants of Home Computer and Mobile Device Security Behavior	Nik Thompson, Tanya Jane McGill, dan Xuequn Wang	2017
11.	Understanding Online Safety Behavior: A Protection Motivation Theory Perspective	Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J. Rifon, dan Shelia R. Cotten	2016
12.	Dampak Penggunaan Broadband Terhadap Perilaku Keamanan Informasi	Dewi Hernikawati	2016

Dari hasil pemilihan literatur yang sesuai dengan topik penelitian dan relevan dalam 5 (lima) tahun terakhir, didapatkan total 12 (dua belas) jurnal yang terdiri dari 3 (tiga) jurnal terbitan tahun 2020, 3 (tiga) jurnal terbitan tahun 2018, 4 (empat) jurnal terbitan tahun 2017, dan 2 (dua) jurnal terbitan tahun 2016.

A. *Kejahatan Dunia Maya (Cyber Crime)*

Kejahatan Dunia Maya (*Cyber Crime*) merupakan salah satu tindakan kriminal yang dilakukan oleh seseorang maupun kelompok orang dengan memanfaatkan internet ataupun komputer [4]. Sedangkan menurut [5], kejahatan siber (*cyber crime*) merupakan salah satu bentuk kriminalitas yang timbul akibat adanya perkembangan *software* pada jaringan internet. Secara umum, kejahatan siber (*cyber crime*) dibagi menjadi 2 (dua) kategori utama, yaitu gangguan ilegal pada jaringan komputer dan gangguan atau penurunan fungsionalitas komputer dan jaringan.

Menurut [6], kejahatan siber (*cyber crime*) dapat terjadi akibat dari penggunaan internet yang kurang bijak dengan besarnya penetrasi internet yang ada, menurutnya, tindakan kriminal rentan terjadi pada dunia maya (*cyberspace*). *Cyberspace* didefinisikan sebagai instrumen elektronik dalam jaringan komputer yang secara dominan digunakan untuk keperluan komunikasi, yang terintegrasi dari berbagai teknologi komunikasi dan jaringan komputer yang dapat menghubungkan seluruh *device* dan tersebar di seluruh dunia [7].

B. *Keamanan Siber (Cyber Security)*

Keamanan Siber (*Cyber Security*) merupakan suatu praktik yang bertujuan untuk melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, maupun data dari berbagai ancaman yang mungkin [8]. Ancaman terhadap keamanan informasi dapat berupa perusakan konfigurasi sistem dan pencurian informasi yang dapat menguntungkan individu [9]. Keamanan siber (*cyber security*) dapat dikatakan sebagai suatu mekanisme yang bertujuan untuk mendeteksi celah dari keamanan sebuah komputer, melakukan pencegahan terhadap ancaman kriminalitas komputer, dan melakukan *recovery* atas komputer maupun perangkat lain yang telah terkena serangan siber (*cyber crime*).

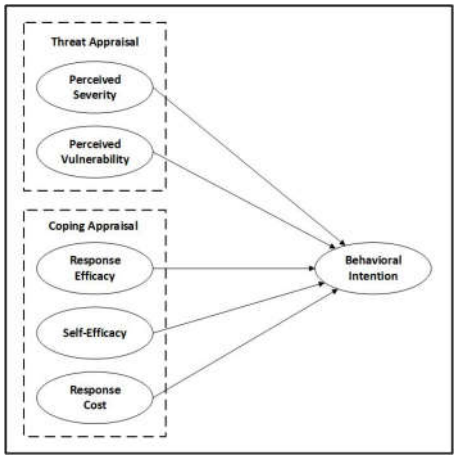
Sekumpulan aktivitas perlindungan terhadap kejahatan siber (*cyber crime*), dapat berupa tindakan teknis maupun non-teknis, yang dimaksudkan untuk melindungi perangkat (*devices*), perangkat lunak (*software*), maupun informasi atau data [10]. Tindakan pengamanan terhadap kejahatan siber merupakan bagian terpenting dari pemanfaatan teknologi, hal ini dilakukan dengan tujuan agar lebih bijak dalam menggunakan teknologi dan dapat meminimalisir adanya penyalahgunaan teknologi tersebut [11].

C. *Protection Motivation Theory (PMT)*

Protection Motivation Theory (PMT) merupakan sebuah teori yang dikemukakan pada tahun 1975 oleh Roger, yang digunakan untuk memahami dampak atau pengaruh yang muncul akibat ketakutan terhadap perubahan pada tingkah laku [12]. *Protection Motivation Theory* (PMT) digunakan dalam proses penilaian terhadap suatu ancaman dan tanggapan atau persepsi yang dapat memunculkan intensi atau minat seseorang dalam melakukan suatu tindakan. Sebagian besar *Protection Motivation Theory* (PMT) pada awalnya digunakan pada bidang kesehatan, namun seiring berjalannya waktu, *Protection Motivation Theory* (PMT) juga digunakan untuk bidang-bidang penelitian yang lain, seperti etiologi, perawatan mandiri, dan perilaku risiko serta perlindungan [12] [13].

Protection Motivation Theory (PMT) melakukan proses penilaian persepsi individu melalui 2 (dua) proses, yaitu *threat appraisal* dan *coping appraisal*. *Protection Motivation Theory* (PMT) berpendapat bahwa ketika individu dihadapkan pada sebuah risiko, maka persepsi dan perilaku individu dalam menanggapi atau merespon risiko tersebut dimotivasi oleh *threat appraisal* dan *coping appraisal* [14].

Pada proses *threat appraisal*, dilakukan sebuah pengukuran atau penilaian terhadap tingkat keparahan suatu ancaman (*perceived severity*) dan persepsi individu terkait kerentanannya terhadap suatu ancaman tertentu (*perceived vulnerability*), sedangkan pada proses *coping appraisal*, dilakukan sebuah penilaian terhadap persepsi individu dalam memutuskan apakah tindakan tertentu terbukti efektif dalam melindungi dari ancaman (*response efficacy*), apakah individu tersebut mampu dalam melakukan tindakan perlindungan dari ancaman (*self-efficacy*), dan apakah usaha yang dikeluarkan dalam melakukan tindakan perlindungan sepadan dengan hasil yang dirasakan (*perceived cost*).



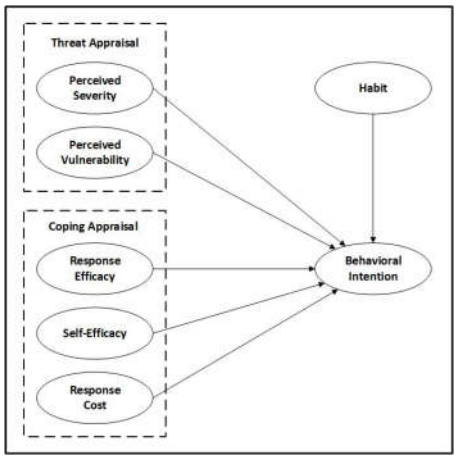
Gambar 1. *Protection Motivation Theory* (PMT)

(Sumber: R. E. Crossler et al., 2009)

D. *Extended-Protection Motivation Theory (PMT)*

Model *Protection Motivation Theory* (PMT) memiliki 5 (lima) variabel yang terdiri atas 2 (dua) proses penilaian, yaitu variabel *perceived severity* dan *perceived*

vulnerability yang berada pada proses *threat appraisal* dan variabel *response efficacy*, *self-efficacy*, dan *response cost* yang berada pada proses *coping appraisal*. Pada kajian literatur ini, ditambahkan variabel yang diduga memiliki pengaruh dalam konteks ini, yaitu variabel *Habit* atau kebiasaan. Sehingga, model konseptual dapat digambarkan melalui Gambar 2 sebagai berikut :



Gambar 2. *Extended-Protection Motivation Theory* (PMT)

(Sumber: Dokumen Pribadi)

E. *Aspek-aspek dari Cyber Security yang Mempengaruhi Adopsi Teknologi*

1) *Perceived Severity*: *Perceived Severity* merupakan persepsi seseorang terkait tingkat keparahan dari suatu ancaman, dalam hal ini adalah ancaman yang berasal dari kejahatan siber (*cyber crime*), yang dapat memberikan dampak atau akibat yang buruk dan merugikan. *Perceived Severity* didefinisikan sebagai tingkat keparahan dari suatu ancaman, yang mana memiliki konsekuensi atau dampak yang serius yang merugikan [15] [16] [17], sehingga indikator yang mendukung variabel *Perceived Severity* ini adalah *Seriousness* dan *Consequences*.

Perceived Severity didefinisikan sebagai tingkat keparahan dari suatu ancaman, yang dapat diukur dari tingkat keseriusan (*Seriousness*) dan konsekuensi (*Consequences*) atas keparahan dari suatu ancaman (*Threats*). Tingkat keseriusan (*Seriousness*) merupakan faktor yang menggambarkan sejauh mana suatu ancaman dapat memberikan dampak yang serius terhadap pemanfaatan teknologi. Sedangkan konsekuensi (*Consequences*) merupakan seberapa buruk dan merugikannya suatu konsekuensi yang akan diterima dari ancaman yang dapat terjadi.

TABEL II
HASIL TELAAH VARIABEL PERCEIVED SEVERITY

Pengaruh	Arah Hubungan	Penjelasan
Signifikan	Positif	Tingginya persepsi seseorang terkait keparahan (*severity*) dari suatu ancaman akan cenderung menyebabkan seseorang lebih merasa perlu mengadopsi teknologi sebagai bentuk tindakan perlindungan terhadap kejahatan siber [19] [20].
Tidak Signifikan	-	Berdasarkan kajian *meta-analytic* tidak menunjukkan adanya impresi yang signifikan antara tingkat keparahan dengan intensi mengadopsi teknologi [21] [22].

Perceived Severity digambarkan sebagai tingkat dampak potensial yang dapat terjadi dari suatu ancaman [18]. Tingginya persepsi seseorang terkait keparahan suatu ancaman akan cenderung menyebabkan seseorang merasa perlu untuk meningkatkan kewaspadaan terhadap *cyber crime*, sehingga akan mempengaruhi seseorang dalam mengadopsi teknologi sebagai bentuk tindakan atau perilaku perlindungan [19].

Berdasarkan hasil penelitian yang dilakukan oleh [20], menunjukkan bahwa *Perceived Severity* memberikan pengaruh yang signifikan terhadap intensi perilaku pencegahan dari *cyber crime*. Semakin mereka menganggap parah sebuah ancaman, maka mereka akan cenderung mengadopsi teknologi untuk melakukan perlindungan terhadap *cyber crime*. Namun, terdapat sebuah kajian *meta-analytic* yang mengindikasikan adanya hubungan yang tidak signifikan antara *Perceived Severity* dan *Behavioral Intention* [21] [22].

Hal ini akan menjadi tantangan tersendiri untuk mengetahui bagaimanakah persepi UMKM di Indonesia terkait tingkat keparahan suatu ancaman dalam mempengaruhi mereka untuk mengadopsi teknologi.

2) *Perceived Vulnerability*: *Perceived Vulnerability* merupakan persepsi terkait sejauh mana seorang individu merasa berisiko atau rentan dalam menerima ancaman tertentu. Persepsi ini didasari oleh kesadaran akan tingkat probabilitas yang mungkin terjadi dan tingkat kemungkinan terjadinya risiko [15] [17] [23], oleh karena itu *Perceived Vulnerability* memiliki 2

(dua) indikator yang mempengaruhi, yaitu *Probability* dan *Likelihood Level of Risk*.

Pengukuran variabel *Perceived Vulnerability* dapat dilihat dari tingkat probabilitas (*Probability*) dan level kemungkinan risiko (*Likelihood Level of Risk*). Tingkat probabilitas (*Probability*) merupakan ukuran persepsi dimana seseorang merasa memiliki probabilitas dalam menerima ancaman (*Threats*) atas pemanfaatan teknologi. Sedangkan level kemungkinan risiko (*Likelihood Level of Risk*) merupakan ukuran persepsi dimana seseorang merasa berisiko menerima ancaman (*Threats*) dari pemanfaatan teknologi. Perbedaan dari 2 (dua) indikator ini adalah terletak pada objek yang dimungkinkannya.

Tingkat probabilitas (*Probability*) mengukur kemungkinan ancaman secara lebih luas, sedangkan level kemungkinan risiko (*Likelihood Level of Risk*) mengukur kemungkinan secara lebih detail terkait risiko dari suatu ancaman yang spesifik.

TABEL III
HASIL TELAAH VARIABEL PERCEIVED VULNERABILITY

Pengaruh	Arah Hubungan	Penjelasan
Signifikan	Positif	Persepsi tingkat kerentanan akan mempengaruhi intensi seseorang dalam mengadopsi teknologi ketika mereka telah *aware* terhadap *cyber crime* [19].
Tidak Signifikan	-	Tidak menunjukkan pengaruh yang signifikan antara persepsi tingkat kerentanan dan intensi mengadopsi teknologi [20]. Hal ini dapat terjadi ketika seseorang belum *aware* terhadap *cyber crime*, sehingga memungkinkan tidak adanya perasaan diri sendiri bahwa mereka rentan terhadap *cyber crime*.

Penelitian yang dilakukan oleh [19] menunjukkan bahwa *Perceived Vulnerability* memiliki pengaruh yang signifikan terhadap perilaku intensi mengadopsi teknologi untuk *cyber security*. Namun, penelitian oleh [20] menunjukkan kontradiksi terkait *Perceived Vulnerability*, yang mengindikasikan tidak adanya pengaruh yang signifikan antara *Perceived Vulnerability* dengan *Behavioral Intention*.

Hal ini mengindikasikan bahwa intensi perilaku mengadopsi teknologi ternyata memungkinkan adanya perbedaan persepsi bergantung pada perilaku dan konteksnya.

Variabel ini akan membantu juga dalam mengetahui tingkat *awareness* UMKM di Indonesia terhadap *cyber crime*, khususnya keterampilan UMKM di Indonesia dalam memitigasi risiko, apabila mereka telah aware dengan adanya *cyber crime*, maka mereka akan cenderung memiliki persepsi bahwa mereka berisiko dan rentan terhadap ancaman dari *cyber crime* yang dapat terjadi kapanpun pada UMKM di Indonesia.

Salah satu yang bisa dilakukan UMKM di Indonesia agar *aware* terhadap *cyber crime* adalah dengan memahami orientasi *cyber ethics* (etika siber), yang merupakan tata perilaku dalam penggunaan dunia maya, sehingga UMKM di Indonesia akan dapat membedakan mana yang termasuk pelanggaran etika maupun yang bukan. Selain itu, UMKM di Indonesia juga dapat meningkatkan *awareness* melalui sosialisasi-sosialisasi terkait *cyber security* maupun mengikuti *Cyber Security Awareness Training* (CSAT).

3) *Response Efficacy*: *Response Efficacy* merupakan suatu tingkat efektivitas yang dirasakan oleh seorang individu atas sebuah perilaku yang dilakukan terkait *cyber security*. Seorang individu akan memiliki kecenderungan untuk mengadopsi teknologi tertentu apabila mereka merasa bahwa hal tersebut mampu melindungi mereka dari *cyber crime* [24].

Response Efficacy dapat didefinisikan sebagai tingkat efektivitas dan manfaat yang dirasakan atas fungsionalitas suatu aktivitas [14] [15] [17], oleh sebab itu terdapat 2 (dua) indikator yang mendukung variabel *Response Efficacy*, yaitu *Effectiveness* dan *Usefulness*.

Tingkat efektivitas (*Effectiveness*) merupakan indikator yang dapat mendukung pengukuran tingkat efektivitas tanggapan yang telah dilakukan dalam pengadopsian teknologi, sejauh mana tanggapan atau respon yang dilakukan telah sesuai dengan kebutuhan mereka. Sedangkan tingkat kegunaan (*Usefulness*) merupakan indikator yang dapat menunjukkan manfaat atas tanggapan yang dilakukan dalam mengadopsi teknologi, seseorang akan merasa bahwa suatu teknologi memberikan manfaat apabila hal tersebut dapat memenuhi kebutuhan atau keperluan seseorang ketika mengadopsi teknologi.

TABEL IV
HASIL TELAAH VARIABEL RESPONSE EFFICACY

Pengaruh	Arah Hubungan	Penjelasan
Signifikan	Positif	Persepsi tingkat efektivitas respon dapat mempengaruhi intensi seseorang dalam mengadopsi teknologi [19] [25]. Seseorangcenderung akan memiliki intensi untuk mengadopsi teknologi ketika mereka merasa bahwa teknologi tersebut secara efektif dapat memberikan manfaat yang sesuai dengan kebutuhan mereka.

Berdasarkan referensi [25] dalam penelitiannya menunjukkan bahwa *Response Efficacy* memiliki pengaruh yang signifikan terhadap *Behavioral Intention*. Sejalan dengan penelitian tersebut, [19] juga menunjukkan adanya pengaruh yang positif antara *Response Efficacy* dengan *Behavioral Intention*.

Response Efficacy dapat dijadikan sebagai tolak ukur terkait sejauh mana UMKM di Indonesia dapat melakukan adopsi teknologi dari sudut pandang *cyber security*. Apabila mereka belum merasa memiliki keterampilan yang cukup, maka perlu adanya semacam training untuk membantu UMKM di Indonesia agar *aware* terhadap *cyber crime*.

4) *Self-Efficacy*: *Self-Efficacy* merupakan keyakinan atas seorang individu terhadap kemampuannya sendiri dalam melakukan perilaku tertentu untuk mencapai tujuan tertentu. Dalam konteks ini, *Self-Efficacy* diartikan sebagai tingkat keyakinan individu [15] [23] terhadap kemampuannya sendiri dalam mengadopsi teknologi kaitannya dengan *cyber security*. Dari definisi tersebut, dapat diketahui bahwa indikator yang mendukung variabel *Self-Efficacy* adalah *Confidence* dan *Self-Capability*.

Tingkat kepercayaan diri (*Confidence*) diasumsikan dapat menjadi salah satu faktor yang mendukung variabel *Self-Efficacy*. *Self-Efficacy* akan dapat dilihat melalui sejauh mana seseorang memiliki persepsi bahwa mereka telah percaya kepada diri mereka sendiri untuk mengadopsi teknologi. Sedangkan tingkat kemampuan diri (*Self-Capability*) merupakan ukuran untuk melihat sejauh mana seseorang merasa bahwa mereka memiliki kemampuan dalam diri mereka untuk mengadopsi teknologi.

TABEL V
HASIL TELAAH VARIABEL SELF-EFFICACY

Pengaruh	Arah Hubungan	Penjelasan
Signifikan	Positif	Persepsi tingkat kepercayaan diri juga dinilai dapat mempengaruhi intensi seseorang dalam mengadopsi teknologi [14] [19]. Tingginya tingkat kepercayaan diri seseorang akan dapat memunculkan intensi dalam mengadopsi teknologi. Seseorang merasa percaya pada kemampuan dirinya sendiri dalam mengadopsi teknologi sejalan dengan tingginya intensi mengadopsi teknologi.

Self-Efficacy menjadi variabel yang memiliki pengaruh yang signifikan terhadap *Behavioral Intention* [14] [19]. Seseorang yang memiliki kepercayaan diri dalam mengadopsi teknologi akan memiliki intensi yang tinggi dalam melakukannya, sehingga hubungan kedua variabel ini adalah signifikan positif.

Variabel ini dapat membantu UMKM di Indonesia untuk mengetahui sejauh mana kemampuan mereka dalam mengadopsi teknologi. Dalam konteks *Cyber Security*, kemampuan mereka dalam mengadopsi teknologi dapat ditinjau dari sejauh mana mereka memiliki pemahaman terkait etika berteknologi, *threat-awareness*, dan kemampuan pemahaman terkait kebijakan serta peraturan dalam berteknologi.

5) *Response Cost*: *Response Cost* merupakan persepsi terkait seberapa bermanfaat suatu perilaku yang dilakukan dengan usaha atau biaya yang dikeluarkan. *Cost* dalam hal ini dapat dibagi menjadi 2 (dua) prinsip, yaitu ekonomi dan non-ekonomi. Prinsip ekonomi yaitu terkait pengeluaran dalam bentuk biaya, seperti modal. Sedangkan prinsip non-ekonomi dapat berbentuk waktu yang dibebankan dan usaha, seperti tingkat kesusahan maupun tingkat kebingungan dalam melakukan adopsi teknologi tertentu [2]. Variabel *Response Cost* didukung oleh 3 (tiga) indikator, yaitu *Money*, *Time*, dan *Effort*.

Cost dalam arti yang umum merupakan suatu biaya yang dikeluarkan untuk aktivitas tertentu. Namun, dalam konteks ini, *Cost* diartikan sebagai besaran yang memuat 3 (tiga) indikator yang mendukungnya, yaitu Biaya (*Money*), Waktu (*Time*),

dan Usaha (*Effort*). Biaya (*Money*) diukur melalui sejauh mana biaya, dalam bentuk materi, akan sebanding dengan manfaat atau kegunaan dari tanggapan atau respon dalam mengadopsi teknologi. Waktu (*Time*) akan mengukur variabel berdasarkan besaran waktu yang harus diluangkan untuk mengadopsi teknologi, apakah sebanding dengan manfaat yang akan dirasakan atau tidak. Sedangkan Usaha (*Effort*) merupakan ukuran seberapa besar usaha yang diperlukan atau dikerahkan dari suatu tanggapan atau respon dalam mengadopsi teknologi.

TABEL VI
HASIL TELAAH VARIABEL RESPONSE COST

Pengaruh	Arah Hubungan	Penjelasan
Signifikan	Negatif	Persepsi terhadap biaya yang dikeluarkan mempengaruhi intensi seseorang dalam mengadopsi teknologi [14]. Apabila biaya yang dikeluarkan lebih sedikit, maka intensi untuk mengadopsi teknologi akan meningkat.
Tidak Signifikan	Negatif	Biaya yang dikeluarkan tidak menunjukkan pengaruh yang signifikan terhadap intensi mengadopsi teknologi [19]. Hal ini dapat terjadi karena perbedaan tujuan dan konteks dari penggunaan teknologi.

Response Cost secara negatif menunjukkan impresi yang signifikan [14]. Namun, penelitian yang dilakukan oleh [19], justru tidak menunjukkan pengaruh yang signifikan meskipun menunjuukan arah yang sama, yaitu negatif. Hal ini dapat terjadi karena perbedaan konteks dan tujuan atas perilaku pengadopsian teknologi tersebut. Sehingga, hasil signifikansi akan berbeda-beda tiap penelitian dengan konteks yang berbeda.

Menarik untuk dapat diteliti terkait bagaimana persepsi UMKM di Indonesia dari sudut pandang *Response Cost*. Dari sini muncul dugaan apakah UMKM di Indonesia sudah *aware* terhadap pentingnya *cyber security* sehingga mereka harus berinvestasi didalamnya.

6) *Habit*: *Habit* merupakan suatu tindakan atau perilaku yang dilakukan secara sistematis, yang telah dipelajari untuk menjadi respon otomatis terhadap peristiwa tertentu. Dalam konteks ini, Habit diartikan sebagai kebiasaan seseorang dalam mengenal teknologi untuk mengadopsinya, namun dilihat dari sudut pandang *cyber security*.

Habit dapat didefinisikan sebagai bentuk respon atau tanggapan otomatis yang dapat mengekspresikan identitas seseorang [17]. Habit juga dapat membentuk dan membangun peristiwa perulangan yang menunjukkan kebiasaan yang telah dilakukan secara berulang [26]. Dari definisi tersebut, maka Habit memiliki 3 (tiga) indikator yang dapat mendukungnya, yaitu *History of Repetition*, *Automaticity*, dan *Expressing Identity*.

Habit atau kebiasaan dapat diukur melalui seberapa sering seseorang dalam mengulang aktivitas-aktivitas di masa lampau (*History of Repetition*), pengulangan ini akan dapat menjadi kebiasaan yang akan mempengaruhi seseorang dalam melakukan tanggapan atau respon atas ancaman (*Threats*) dalam mengadopsi teknologi. *Habit* atau kebiasaan juga dapat diukur melalui informasi psikologi, dimana seseorang yang telah terbiasa akan menjadikan kebiasaan tersebut sebagai tanggapan otomatis yang tanpa memerlukan proses kognitif yang lebih panjang dalam membuat suatu keputusan (*decision making*).

Dalam konteks ini, *Automaticity* akan memberikan pengaruh kepada seseorang dalam menentukan apakah mereka akan mengadopsi teknologi atau tidak, melalui kebiasaan-kebiasaan yang telah dilakukan. Pengukuran *Habit* atau kebiasaan juga dapat dilihat dari bagaimana mereka mengekspresikan identitas diri terhadap tanggapan atau respon dari suatu ancaman (*Threats*) dalam mengadopsi teknologi melalui kebiasaan-kebiasaan yang telah dilakukan.

TABEL VII
HASIL TELAAH VARIABEL HABIT

Pengaruh	Arah Hubungan	Penjelasan
Signifikan	Positif	*Habit* atau kebiasaan menunjukkan pengaruh yang signifikan terhadap intensi mengadopsi teknologi [27]. Seseorang akan cenderung memiliki intensi ketika mereka telah terbiasa dengan ancaman-ancaman (*threats*) dari *cyber crime* [17]. Seseorang tidak akan memiliki kecenderungan dalam mengadopsi teknologi ketika mereka belum *aware* terhadap kemungkinan ancaman dari *cyber crime*.

Penelitian terdahulu yang dikerjakan oleh [27] mengindikasikan bahwa *Habit* memiliki impresi yang signifikan terhadap *Behavioral Intention* untuk mengadopsi teknologi. Dari penelitian yang dikembangkan oleh [17], *Habit* menjadi salah satu proses kognitif penting yang memberikan pengaruh terhadap intensi perilaku dalam mengadopsi teknologi melalui *cyber security awareness*.

UMKM di Indonesia perlu menumbuhkan kebiasaan untuk *aware* terhadap *cyber security*, sehingga proses adaptasi untuk adopsi teknologi akan semakin mudah, melalui kebiasaan-kebiasaan yang telah dilakukan sebelumnya secara sistematis, otomatis, dan tanpa proses kognitif yang lebih panjang.

III. KESIMPULAN

Persepsi UMKM di Indonesia terhadap *Cyber Security* dalam intensi untuk mengadopsi teknologi perlu dilakukan penelitian, agar dapat menjadi tolak ukur UMKM di Indonesia untuk mengetahui kapabilitas dan kemampuan mereka dalam mengadopsi teknologi dari sudut pandang *cyber security*. Dari hasil telaah literatur, didapatkan beberapa faktor-faktor yang mungkin dapat mempengaruhi UMKM di Indonesia dalam mengadopsi teknologi, namun diturunkan melalui sudut pandang *cyber security*. Pengambilan faktor-faktor ini didasarkan dari penelitian-penelitian terdahulu yang searah dengan konteks penelitian dan relevan, serta objek dalam penelitian ini, yaitu UMKM di Indonesia. Karena konteks dalam penelitian ini adalah tentang persepsi, sehingga hasil yang didapatkan nantinya bisa jadi berbeda dengan hasil penelitian yang lain.

Penelitian ini mengadopsi model *Protection Motivation Theory* (PMT). Sehingga, faktor yang dapat mempengaruhi intensi UMKM di Indonesia dalam mengadopsi teknologi dari sudut pandang *cyber security*, antara lain variabel *Perceived Severity* yang memiliki indikator *Seriousness* dan *Consequences*, memunculkan asumsi bahwa semakin tinggi tingkat keparahan yang dirasa atas suatu ancaman, maka juga akan meningkatkan minat atau intensi dalam mengadopsi teknologi. Indikator *Probability* dan *Likelihood Level of Risk* dari variabel *Perceived Vulnerability* juga memunculkan asumsi bahwa semakin seseorang merasa rentan dan berisiko untuk terkena ancaman *cyber crime*, maka semakin tinggi minat atau intensi seseorang dalam mengadopsi teknologi. Variabel *Response Efficacy* memiliki indikator *Effectiveness* dan *Usefulness*, yang memunculkan asumsi bahwa tingkat keefektivan dan kegunaan suatu teknologi akan mempengaruhi minat atau intensi dalam mengadopsi teknologi tersebut. Begitu juga dengan variabel *Self Efficacy* yang memiliki indikator *Confidence* dan *Self-Capability*, menunjukkan asumsi bahwa minat atau intensi untuk mengadopsi teknologi akan meningkat seiring dengan tingginya persepsi seseorang dalam memahami kemampuan dan kepercayaan diri mereka. Variabel *Response Cost* yang memiliki indikator *Money*, *Time*, dan *Effort*, menunjukkan asumsi bahwa seseorang akan cenderung memiliki minat atau intensi mengadopsi teknologi, apabila seluruh usaha dan biaya yang dikeluarkan sesuai dan sebanding dengan manfaat yang diharapkan. Selain itu, dilakukan penambahan variabel *Habit* yang memiliki indikator *History of Repetition*, *Automaticity*, dan *Expressing Identity*, dengan asumsi bahwa tingkat intensi seseorang juga dapat dipengaruhi oleh *Habit* atau kebiasaan. Asumsinya, seseorang akan cenderung memiliki minat atau intensi ketika mereka telah terbiasa dalam mengadopsi teknologi.

Dari penelitian ini, akan dapat memunculkan hipotesis-hipotesis yang diharapkan dapat menunjukkan kebenaran asumsi yang telah dipaparkan, sehingga dari hasil analisis lebih lanjut akan dapat diketahui terkait faktor-faktor dari perspektif *cyber security* apa saja yang secara signifikan dapat mempengaruhi UMKM di Indonesia untuk mengadopsi teknologi.

UCAPAN TERIMA KASIH

Penyelesaian artikel ilmiah ini tentunya tidak terlepas dari dukungan dan doa dari beberapa pihak. Oleh karena itu, penulis mencoba mengucapkan terimakasih kepada:

1. Bapak Rahadian Bisma, S.Kom., M.Kom. sebagai dosen pembimbing skripsi yang telah meluangkan waktu untuk memberikan arahan dan bimbingan, serta membagikan ilmu kepada penulis sehingga artikel ilmiah ini dapat terselesaikan
2. Kedua orang tua yang senantiasa memberikan dukungan dan doa
3. Bapak dan Ibu Dosen Penguji yang telah berkenan memberikan saran dan membagikan ilmu dalam penyelesaian artikel ilmiah ini
4. Seluruh teman-teman yang saling memberikan dukungan dan semangat dalam penyelesaian artikel ilmiah ini

REFERENSI

[1] Utami, R., & Baihaqi, W. M. (2020). Pengaruh Teknologi Informasi Revolusi Industri 4 . 0 terhadap Perkembangan UMKM Sektor Industri Pengolahan. 10(3), 87–93.

[2] Hanum, A. N., & Sinarasri, A. (2017). Analisis faktor-faktor yang mempengaruhi adopsi e commerce dan pengaruhnya terhadap kinerja umkm (studi kasus umkm di wilayah kota semarang). Maksimum Media Akuntansi, Vol. 1(No. 1), 1–15.

[3] Kent, C., Tanner, M., & Kabanda, S. (2016). How South African SMEs address cyber security: The case of web server logs and intrusion detection. 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies, EmergiTech 2016, 100–105. https://doi.org/10.1109/EmergiTech.2016.7737319

[4] Fitriana, M., AR, K., & Marsya, J. M. (2020). PENERAPANA METODE NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY (NIST) DALAM ANALISIS FORENSIK DIGITAL UNTUK PENANGANAN CYBER CRIME. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 4(1), 29–39. https://doi.org/10.22201/fq.18708404e.2004.3.66178

[5] Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. Jurnal Pertahanan & Bela Negara, 7(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193
[6] Putra, B. K. B. (2019). Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia. Pamulang Law Review, 1(1), 1. https://doi.org/10.32493/palrev.v1i1.2842
[7] Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. E3S Web of Conferences, 125(201 9), 1–5. https://doi.org/10.1051/e3sconf/201912521001
[8] Rahmadi, G. (2019). Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia.
[9] Rif, S., & Bisma, R. (2021). Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO / IEC 27001 : 2013 pada institusi pemerintah Gap analysis of information security management system (ISMS) in preparation for ISO / IEC 27001 : 2013 cert. 11(1).
[10] Blythe, J. M., Coventry, L., & Little, L. (2019). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security, 103–122.
[11] Hidayat, A. N. (2020). Peningkatan Cyber Security Dengan Penerapan Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001:2005. In Teknik Elektro Universitas Mercu Buana Jakarta.
[12] Hernikawati, D. (2016). Desain Penelitian Dampak Penggunaan broadband terhadap perilaku Keamanan Informasi. Jurnal Studi Komunikasi Dan Media, 20(1), 77. https://doi.org/10.31445/jskm.2016.200105
[13] Yusmita, F., & Evayani, E. (2020). Pentingnya Sistem Informasi Akuntansi Yang Handal Terhadap Bencana Pada Sektor Pemerintahan. Jurnal Ilmiah Mahasiswa Ekonomi Akuntansi, 5(1), 1–11. https://doi.org/10.24815/jimeka.v5i1.15493
[14] Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. Computers and Security, 77, 860–870. https://doi.org/10.1016/j.cose.2018.03.008
[15] Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040
[16] Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective. Journal of the Association for Information Systems, 11(7), 394–413.
[17] Tsai, A. H. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., Cotten, S. R., Rifon, N. J., & Cotten, S. R. (2016). Understanding Online Safety Behaviors : A Protection Motivation Theory Perspective Hsin-yi Sandy Tsai , PhD , Assistant Professor # Mengtian Jiang , PhD Student † Saleem Alhabash , PhD , Assistant Professor *† Robert LaRose , PhD , Professor *. Computers & Security. https://doi.org/10.1016/j.cose.2016.02.009
[18] Hassandoust, F. (2020). Chapter 7 - Understanding users' information security awareness and intentions: a full nomology of protection motivation theory11The previous version of this paper was published in the Proceedings of the 22nd Pacific Asia Conference on Information Sy. In Cyber Influence and Cognitive Threats (Issue June 2018). Elsevier Inc. https://doi.org/10.1016/B978-0-12-819204-7.00007-5
[19] Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. Computers in Human Behavior. https://doi.org/10.1016/j.chb.2018.05.023
[20] Jansen, J., & Schaik, P. van. (2017). Comparing Three Models to Explain Precautionary Online Behavioural Intentions. Information & Computer Security, 25(2). https://doi.org/10.1108/ICS-03-2017-0018
[21] April, Y., Sari, L., Kusyanti, A., & Rokhmawati, R. I. (2018). Analisis Faktor-Faktor yang Memengaruhi Perilaku Pengguna Sistem Informasi Akademik Mahasiswa dalam Penciptaan Kata Sandi Kuat dengan Menggunakan Protection Motivation Theory (Studi pada XYZ). Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya, 2(4), 1348–1357.
[22] Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. Journal of Applied Social Psychology, 30(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x
[23] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers and Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007
[24] Almarshad, S. O. (2017). Adopting Sustainable Behavior in Institutions of Higher Education: a Study on Intentions of Decision Makers in the Mena Region. European Journal of Sustainable Development, 6(2), 89–110. https://doi.org/10.14207/ejsd.2017.v6n2p89
[25] Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. Data Base for Advances in Information Systems, 45(4), 51–71. https://doi.org/10.1145/2691517.2691521
[26] Verplanken, B., & Orbell, S. (2003). Reflections on Past Behavior: A Self-Report Index of Habit Strength. Journal of Applied Social Psychology, 33(6), 1313–1330. https://doi.org/10.1111/j.1559-1816.2003.tb01951.x
[27] Aigbefo, Q. A., Blount, Y., & Marrone, M. (2020). The influence of hardiness and habit on security behaviour intention. Behaviour and Information Technology, 0(0), 1–20. https://doi.org/10.1080/0144929X.2020.1856928
[28] Crossler, R. E., Bélanger, F., Brown, R. M., Fan, W., Hiller, J. S., & Sheetz, S. D. (2009). Protection Motivation Theory: Understanding the Determinants of Individual Security Behavior Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Doct.