Cendekia Niaga
Journal of Trade Development and Studies
p-ISSN 2548-3137, e-ISSN 2548-3145

Upaya Membangun Kesadaran Keamanan Siber pada Konsumen *E-commerce* di Indonesia

Ratri Nur Rohmah
Pusdiklat Badan Siber dan Sandi Negara

Email : ratri.nih@gmail.com

Abstrak

Perkembangan teknologi informasi dan komunikasi telah mengubah perilaku masyarkat dalam melakukan transaksi jual beli. Dengan munculnya *e-commerce* maka kebiasaan belanja konsumen yang semula bersifat konvensional beralih ke *e-commerce*. Namun demikian, dengan transaksi pada *e-commerce* tidak hanya memberikan dampak positif namun juga menimbulkan dampak negatif. Salah satu bentuknya adalah munculnya kerugian di kalangan konsumen *e-commerce* akibat adanya kejahatan di dunia siber. Oleh karena itu konsumen sebagai pelaku *e-commerce* perlu untuk dilindungi dan diamankan. Pengamanan di dunia siber tidak hanya perangkat yang diperkuat, namun sumber daya manusia juga perlu diberikan pemahaman tentang kesadaran keamanan siber. Oleh karena itu, penelitian ini bertujuan untuk mengetahui program kesadaran keamanan siber yang dapat dibangun untuk melindungi konsumen *e-commerce*. Metode yang digunakan adalah analisis deskriptif berdasarkan data yang diperoleh berdasarkan pengamatan, wawancara serta dokumen yang relevan dengan tema penelitian. Hasil dari penelitian menunjukkan bahwa upaya membangun kesadaran keamanan siber di kalangan konsumen *e-commerce* dapat dilakukan melalui program *awareness* atau program kesadaran keamanan siber. Program *awareness* ini sangat sederhana dan tidak terlalu formal. Dalam penerapannya perlu disiapkan beberapa aspek seperti struktur, prioritas, materi, penyajian dan penganggarannya. Materi yang dipilih diupayakan dapat menyentuh langsung pada pengguna yaitu pelaku *e-commerce*. Di sisi lain juga diperlukan dukungan dari penyedia *market place* untuk mengkampanyekan program kesadaran keamanan siber ini. Agar program ini dapat berjalan dengan baik, maka diperlukan evaluasi yang dilakukan secara terus menerus terhadap upaya pembangunan kesadaran keamanan siber ini.

Kata Kunci : keamanan siber, kesadaran keamanan siber, e-commerce

Abstract

Technological developments change people's behavior in buying and selling transactions. Consumer's shopping habits switched to e-commerce. However, transactions in e-commerce not only have a positive impact but also have a negative impact. consumers suffer losses due to cybercrime. Consumers need security. Cyber security is not only a device, but also human needs to provide an understanding of cyber security awareness. This study aims to determine the cybersecurity awareness program that can be built to protect e-commerce players. The method used is descriptive analysis conducting a literature study based on references. The results of the study indicate that efforts to build cybersecurity awareness among e-commerce players can be carried out through awareness programs or cybersecurity awareness programs. This awareness program is very simple and not too formal. It is necessary to prepare several aspects such as structure, priorities, materials, presentation and budgeting. The selected material can be searched directly for users, namely e-commerce actors. On the other hand, support from market providers is also needed to campaign for this cyber security awareness program. It is also necessary to carry

out continuous evaluation of this cybersecurity awareness building effort to get feedback for improvement.

Keywords: cyber security, awareness, e-commerce,

PENDAHULUAN

E-commerce

Perkembangan teknologi informasi dan komunikasi yang pesat mempermudah informasi untuk dapat diakses dari mana saja dan kapan saja. Internet yang merupakan jaringan komputer raksasa telah menghubungkan seluruh titik di berbagai negara. Inilah yang menjadi cikal bakal arus Informasi sangat mudah untuk didapatkan bahkan pada saat harus melewati batas wilayah dan negara sekalipun.

Perkembangan teknologi informasi dan komunikasi ini memberikan dampak yang signifikan dalam mengubah wajah dunia. Salah satu dampak yang terasa adalah pengurangan pemanfaatan kertas (*paperless*) dalam berbagai bidang termasuk bidang ekonomi. Transaksi tidak lagi menggunakan kertas sebagai media koordinasi, perjanjian dagang maupun bukti transaksi. Namun saat ini sudah digantikan dengan media digital seperti dengan memanfaatkan *email, chat*, termasuk pembayaran yang dilakukan secara digital.

Berbagai kemudahan bertransaksi dalam bentuk digital telah menggerakkan perdagangan secara *online* atau yang sering dikenal dengan *e-commerce* ini semakin populer dan disukai masyarakat. Bahkan, saat ini banyak perusahaan berbasis teknologi yang memegang peran pasar dalam industri dan perdagangan.

Adapun pengertian *e-commerce* (Kotler&Amstrong, 2012) adalah saluran *online* yang dapat dijangkau seseorang melalui komputer, yang digunakan oleh pebisnis dalam melakukan aktifitas bisnisnya dan digunakan konsumen untuk mendapatkan informasi dengan menggunakan bantuan komputer yang dalam prosesnya diawali dengan memberi jasa informasi pada konsumen dalam penentuan pilihan. Menurut ahli lain (Wong, 2010) mengungkapkan bahwa *e-commerce* proses jual beli dan memasarkan barang serta jasa melalui sistem elektronik, seperti radio, televisi dan jaringan komputer atau internet.

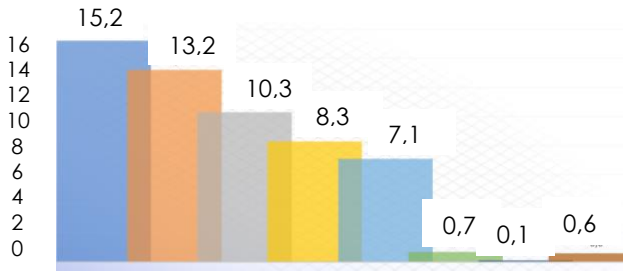
Salah satu kemudahan dalam transaksi perdagangan adalah tersedianya berbagai macam barang kebutuhan yang tersedia dan ditawarkan dengan berbagai macam pilihan model, mutu maupun harga. Berbagai jenis barang tersebut yang tersedia juga sangat beragam mulai dari barang kebutuhan sehari-hari, kebutuhan kantor, barang untuk kesenangan atau hobi dan sebagainya. Barang tersebut kemudian ada yang dikelompokkan dalam produk seperti fashion, kecantikan, pangan, kesehatan, rumah tangga, kebutuhan pendidikan, film dan video, elektronik, aksesoris kendaraan, hotel dan penginapan, tiket, games, musik dan sebagainya.

Besarnya transaksi melalui *e-commerce* sangat luar biasa. Trend ini berlaku hampir di seluruh negara di dunia, termasuk negara maju seperti Amreika Serikat. Seperti pernyataan salah seorang pemimpin dalam ekonomi digital Amerika Serikat bahwa di negara Amerika Serikat telah berhasil mengumpulkan pendapatan USD 5,9 triliun melalui ekonomi digital yang setara dengan 33% Domestik Bruto Produk (PDB) (Teoh & Mahmood, 2017).

Banyaknya transaski melalui *e-commerce* ini juga dapat dilihat berdasarkan nominal uang yang dikeluarkan untuk berbelanja pada *platform* digital. Sesuai data (Irawan et al., 2020) di Indonesia sebagian besar (43,2%) masyarakat melakukan belanja secara *online* di *e-commerce* dengan nominal pengeluaran antara satu juta hingga dua juta rupiah dalam satu bulan. Bahkan berdasarkan data dari sumber yang sama, ada pula golongan masyarakat yang melakukan kebiasaan

belanja secara *online* lebih dari sepuluh juta rupiah per bulan. Tentunya hal ini bukan jumlah yang sedikit dan menjadi isu yang patut untuk diperhatikan.

Terdapat beberapa alasan yang menyebabkan konsumen semakin menggemari berbelanja secara *online*. Berdasarkan survei yang dilakukan APJII terdapat berbagai alasan yang menyebabkan peningkatan jumlah konsumen Indonesia berbelanja pada e-commerce. Alsan tersebut seperti disajikan pada Gambar 1 berikut:



Gambar 1
Sumber : APJII (Irawan et al., 2020)

Keterangan:
- : Harga jauh lebih murah
- : Belanja dapat dilakukan dimana saja
- : Lebih cepat dan praktis
- : Banyak diskon dan promo
- : Mudah membandingkan barang yang akan dibeli
- : Semua betul
- : Karena Pandemi covid-19
- : Lainnya

Berdasarkan Gambar 1, dapat diketahui berbagai alasan konsumen memilih belanja di *e-commerce*. Berbagai kemudahan yang disajikan pada e-commerce ini akhirnya membentuk kebiasaan baru masyarakat dari yang awalnya bertransaksi secara konvensional kemudian bergeser pada kecenderungan bertransaksi pada platform digital melalui *e-commerce*.

Dalam *e-commerce* tidak hanya konsumen yang dimanjakan, penyedia barang dan jasa juga mendapatkan keuntungan dengan kemunculannya. Kemudahan dalam distribusi barang dan sistem otomatisasi merupakan salah satu hal yang dapat mengurangi biaya operasional penyedia. Seperti yang diungkapkan Widagdo (2016) bahwa keuntungan *e-commerce* bagi pebisnis adalah pengurangan biaya operasional dan dapat memperlebar pangsa pasar, sehingga keuntungan dapat dimaksimalkan dan lebih mudah dalam hal pengembangan bisnis.

Berbagai keuntungan baik bagi penyedia maupun konsumen *e-commerce* ini membuat perdagangan secara *online* ini semakin tumbuh membesar. Bahkan beberapa lembaga di Indonesia telah melakukan prediksi menganai perkembangan pengguna *e-commerce* beberapa tahun ke depan. Gambar 2 berikut ini adalah prediksi pengguna *e-commerce* di Indonesia dari tahun 2017 sampai dengan 2024.

Gambar 2. Prediksi Angka Penggunaa *E-commerce* di Indonesia 2024
Sumber : Tempo (Firdhy Esterina Christy, 2020)

Berdasarkan gambar 2 maka dapat diketahui bahwa jumlah pengguna *e-commerce* selalu mengalami peningkatan dari tahun ke tahun. Pada tahun 2017 tercatat 70,8 juta pengguna e-commerce. Selanjutnya jumlah ini akan terus bertambah dengan prediksi di tahun 2024 akan mencapai 189,6 juta pengguna. Sehingga tidak mustahil jika Indonesia diigadang-gadang akan menjadi pasar e-commerce terbesar di Asia bahkan dunia. (Accurate online, 2018)

Ancaman Keamanan Siber

Berbagai kemudahan yang ditawarkan dalam *e-commerce* tidak hanya memberikan dampak positif. Dampak negatif juga sering muncul di kalangan pengguna akibat adanya celah kerawanan serta ancaman terhadap

customer atau konsumen karena bertransaksi di dunia siber.

Dampak negatif sering dirasakan oleh pengguna khususnya konsumen. Konsumen dalam *e-commerce* ini merupakan para pengguna internet yang dijadikan sebagai target pasar yang potensial untuk diberikan penawaran berupa produk jasa atau informasi oleh para penjual. Sementara itu, untuk melakukan transaksi, konsumen perlu melakukan registrasi maupun pembayaran yang menginput data pribadi yang bersifat konfidensial. Sehingga konsumen inilah yang potensial akan banyak mendapatkan ancaman siber dalam penggunaan *e-commerce* ini.

Beberapa bentuk kejahatan yang dapat dijadikan sebagai target ancaman kejahatan siber pada konsumen *e-commerce* diantaranya dapat berupa:

1. *Data breach,* merupakan insiden keamanan di mana informasi diakses tanpa adanya otorisasi.
2. *Spoofing,* merupakan bentuk penipuan online yang dilakukan dengan cara berpura-pura menjadi sebagai seseorang / pihak tertentu yang biasanya dikenal dan dipercaya oleh korban.
3. *Phising,* merupakan upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang dijadikan sasaran dari kegiatan phising adalah data pribadi, data akun dan data finansial yang dapat berupa nomor rekening maupun kartu kredit, dan lain-lain.

Kasus kebocoran data perah terungkap pada salah satu *platform e-commerce* yang ada di Indonesia. Telah beredar kabar di berbagai media mengenai adanya jual beli data konsumen melali internet. Selain itu kasus penipuan dengan teknik *spoofing* maupun *phising* juga banyak dilaporkan masyarakat pada layanan aduan siber milik pemerintah.

E-commerce menarik untuk dijadikan obyek para penjahat di dunia siber karena ada uang yang beredar pada *platform* ini. Contohnya adalah pada saat konsumen melakukan pembayaran. Metode pembayaran di dalam *e-commerce* tidak hanya dilakukan secara tunai melalui sistem pembayaran *Cash On Delivery*, namun banyak konsumen yang menggunakan metode pembayaran melalui transfer bank, *mobile banking, e-wallet* dan metode pembayaran digital lainnya. Dengan adanya data sensitif di dalam *e-commerce* ini yang selanjutnya menarik penjahat untuk melakukan eksploitasi dengan cara ilegal.

Telah terjadi beberapa kasus yang merugikan korban terutama dari pihak konsumen akibat bertransaksi di dalam *e-commerce*. Hal ini selaras dengan beberapa jenis ancaman yang ada di dunia siber seperti yang telah diidentifikasi (Teoh & Mahmood, 2017) sebagai berikut:

1. *Malware and Zero Day Attack, malicious software* atau yang disingkat malware ini merupakan software jahat yang dapat menginfeksi dan merusak perangkat teknologi informasi yang kita gunakan dalam ranah digital. Malware ini dapat berupa virus, worm, spam, DOS, trojan dan sebgainya. Ancaman ini selalu muncul yang baru yang tidak ditemukan sebelumnya yang dikenal dengan *Zero Day Attack.*
2. *Rampant organized cybercrime*
   Jenis kejahatan siber tidak hanya dilakukan oleh perseorangan namun ada juga yang telah terorganisisasi dengan baik yang dikenal dengan Rampant organized cybercrime.
3. *Personal information and data breach*
   Personal information and data breach ini memang sangat populer. utamanya dalam e-commerce. Data-data pribadi saat melakukan transaksi dapat saja mengalami kebocoran akan sangat merugikan pemiliknya.
4. *States and State-sponsored attack increasingly, state and state sponsored group are targeting the nation network, for political diplomatic, technological, commercial and strategic motives.*
   Kejahatan di dunia siber juga dapat disponsori oleh suatu negara. Jenis kejahatan ini menargetkan jaringan bangsa, untuk motif diplomatik politik, teknologi, komersial dan strategis.
5. *Advanced Persistent Threat (APT)*

Kejahatan ini sudah sangat matang dan terencana dan didukung perangkat yang sangat baik.

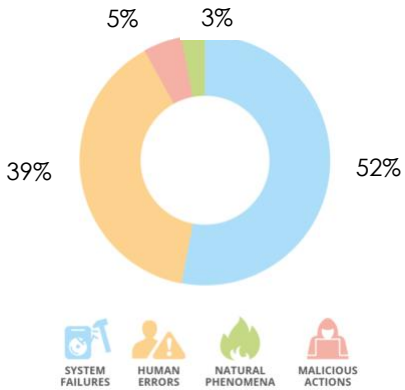
Jenis kejahatan di dunia siber dapat juga dibedakan berdasarkan motif dari pelakunya. Karena pada dasarnya kejahatan tersebut tidak akan terjadi jika pelaku tidak memiliki motif yang mekatarinya. Jenis motivasi pelaku kejahatan siber menurut peneliti (Desman, 2001) diklasifikasikan menjadi beberapa kelompok:

1. alasan uang, pelaku melakukan kejahatan di dunia siber karena keinginannya untuk mendapatkan sejumlah uang.
2. *hacktivism*, pelaku melakukan kejahatan dengan motivasi untuk melakukan propaganda untuk mendapatkan pengikut.
3. *trade secret, dilakukan oleh pelaku untuk mengetahui informasi rahasi dari perusahaan lainnya.*
4. *cyber war, dilakukan untuk memperkuat ketahanan nasional maupun menyerang negara lainnya.*
5. *bragging right, merupakan salah satu motivasi pelaku kejahatan di dunia siber untuk dapat pengakuan dan menyombongkan dirinya.*

Munculnya berbagai ancaman di dunia siber termasuk *e-commerce* ini perlu ditangani yaitu dengan menyiapkan pengamanannya. Adapun pengertian keamanan *e-commerce* (Khan, 2019) adalah perlindungan aset *e-commerce* dari yang tidak sah akses, penggunaan, perubahan, atau penghancuran.

Dengan banyaknya jenis kejahatan ini, pelaku *e-commerce* dapat mengalami kerugian. Slah satu contoh kerugian yang dirasakan konsumen adalah kehilangan uang akibat pembobolan akun pada saat melakukan transaksi secara digital. Pembobolan ini dapat disebabkan karena beberapa hal seperti kekuatan *password* yang kurang, kelalaian dari pihak yang menangani data, kelalaian pengguna, dan sebagainya.

Ada beberapa penyebab yang mengakibatkan munculnya ancaman keamanan siber. Namun demikian penyebab utama munculnya insiden siber sesuai dengan laporan (Report, 2020) meliputi empat hal seperti gambar 3 berikut.



Gambar 3 Laporan Insiden
Sumber: Enisa (Report, 2020)

Berdasarkan gambar 3. dapat diketahui bahwa *human error* menempati urutan ke-dua sebagai salah satu penyebab munculnya ancaman keamanan siber. Sekitar 39% insiden disebabkan oleh kesalahan manusianya. Sementara itu, penyebab terbesar adalah karena System failures yaitu sebesar 53%. Kesalahan ini dapat berupa hardware failures or software bugs.

Adanya berbagai macam ancaman tersebut, maka perlu dilakukan antisipasi untuk pengamanan. Adapun prinsip dalam keamanan dalam dunia siber adalah terpenuhinya tiga unsur sebagai berikut:

1. *Confidentiality*
   Terjaganya kerahahasiaan data
2. *Integrity*
   Keutuhan dan keaslian dari data
3. Authentication
   Keaslian dari *user*/pengguna

.

METODOLOGI

Penelitian ini dilakukan dengan menggunakan metode deskriptif. Data dan informasi dikumpulkan berdasarkan observasi, wawancara maupun dokumen. Hal ini sekaligus untuk menguji keabsahan data berdasarkan

metode triangulasi yang dilakukan yaitu pengecekan data berdasarkan pengamatan yang dilakukan, dibandingkan dengan hasil wawancara serta dokumen/literatur yang telah dikumpulkan. Adapun metode analisis yang dilakukan dengan menerapkan beberapa tahapan yaitu reduksi data, tampilan data, mengambil keputusan dan verifikasi. Reduksi data dilakukan terhadap data yang telah dikumpulkan dan melakukan sortir dengan memilah dan memilih data yang sesuai dengan tema penelitian. Selanjutnya untuk mempermudah analisis, data yang telah disortir akan disajikan dalam bentuk tampilan yang memudahkan untuk analisis sebelum dibuat kesimpulannya. Dengan demikian data tersebut dapat digunakan untuk mengetahui permasalahan mengenai upaya membangun program kemanan siber khusunya pada konsumen *e-commerce* di Indonesia.

HASIL DAN PEMBAHASAN

Kesadaran Keamanan Siber

Sebagaimana yang telah diketahui, bahwa untuk mewujudkan keamanan siber tidak hanya bergantung pada teknologi yang digunakan, namun juga terkait dengan kebijakan maupun sumber daya manusia. Sumber daya manusia menjadi target yang dapat dimanfaatkan kelemahannya oleh para pelaku kejahatan dengan cara mempelajari celah kemungkinan peluang yang ada.

Telah diungkapkan (Rahmadi & Raf'ie Pratama, 2020) bahwa peretas (individu atau kolektif) cenderung mencari pengguna yang paling rentan yaitu mereka yang kurang dalam pengetahuan dan kesadaran keamanan siber Sehingga peningkatan kesadaran keamanan ini penting untuk dilakukan untuk menangani kerawanan maupun ancaman siber saat bertransaksi di dalam *e-commerce*.

Memperhatikan trend di *e-commerce*, maka konsumen yang dominan menjadi pelaku di dalamnya. Terlihat dari data (BPS, 2020) bahwa usaha *e-commerce* menjual barang/jasa ke konsumen akhir secara langsung dibandingkan menjual ke agen atau reseller. Oleh karena itu, peran sumber daya manusia dalam hal ini konsumen *e-commerce* sangat penting untuk dilindungi sekaligus dijadikan sumber daya yang kuat untuk menanggulangi kejahatan siber. Tabel 1. menggambarkan kondisi umum kesenjangan terkait pemahaman tentang keamanan siber pada konsumen *e-commerce*.

Tabel 1. Kesenjangan pemahaman tentang keamanan siber pada konsumen *e-commerce*.

Kondisi saat ini	**Kondisi Ideal**	**Pemecahan masalah**
konsumen belum memahami bahaya yang mengancam saat bertransaksi digital di e-commerce	Konsumen menyadari adanya ancaman saat bertransaksi digital di e-commerce	Program Security awareness
Konsumen belum memahami langkah antisipasi untuk pengamanan saat bertransaksi di e-commerce	Konsumen mengetahui langkah yang harus dilakukan agar dapat bertransaksi digital di e-commerce secara aman	Program Security awareness

Salah satu program yang dapat diterapkan untuk mewujudkan keamanan siber adalah dengan memberikan pemahaman tentang kesadaran keamanan siber atau security awareness. Dengan demikian konsumen *e-commerce* sebagai *end user* dapat selalu waspada terhadap bahaya ancaman siber. Hal ini sejalan dengan yang diungkapkan (Rahmadi & Raf'ie Pratama, 2020) bahwa keamanan siber dapat dibagi menjadi beberapa kategori umum seperti *network security, information security, dan end-user education.*

Upaya kesadaran keamanan siber sendiri didesain untuk mengubah kebiasaan agar dapat menerapkan keamanan siber yang baik (NIST 800-50, 2003). Kesadaran kemanan ini diartikan dalam NIST *Special Publication* 800-16 sebagai berikut: "*Awareness is not training. The purpose of awareness presentations is simply to*

focus attention on security." Kesadaran kamanan siber ini diharapkan dapat mengajak setiap individu untuk mampu mengenal kemanan siber dan merespon dengan baik.

Dengan demikian konsumen *e-commerce* dapat peduli terhadap kemanannya sendiri saat berada di dalamnya. Sesuai dengan yang diungkapkan seorang peneliti (Kristian Angelo et al., 2014) yang merekomendasikan bahwa "*the online shoppers should have their own initiative to take care of their own personal information and the online shoppers must also be aware of the hackers. Never log in your account in a pop-up window and be aware of scams that are being sent in your email.*"

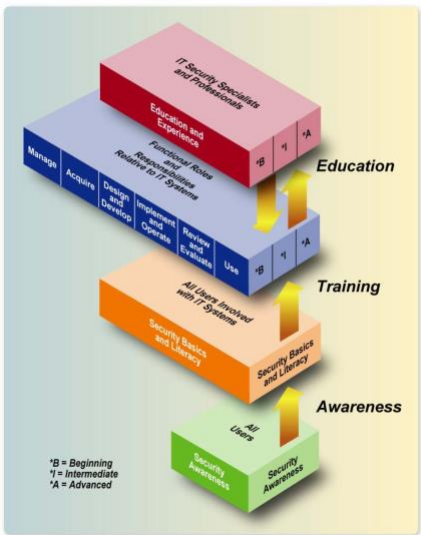
Salah satu upaya riil yang dapat dilakukan untuk membangun kesadaran kemanan siber ini adalah dengan memberikan edukasi berupa literasi digital terkait konten materi keamanan siber kepada konsumen *e-commerce*.

Program Kesadaran Keamanan Siber

Berdasarkan (NIST, 2003) terdapat beberapa komponen dalam membangun kesadaran keamanan siber yaitu:

a. *Awareness* seperti yang diungkap sebagai berikut: "*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly*."
   Di dalam kegiatan *awareness* ini masayarakat sebagai pembelajar yang menerima informasi tentang keamanan siber dan yang lebih aktif. Dalam awareness ini materi kesadaran keamanan dapat disebarluskan dengan sederhana dan teknik penyajian yang menarik. Adapun materi yang disampaikan biasa dikenal dengan materi dasar keamanan dan literasi.
b. *Training*, biasanya bersifat lebih formal dan tujuannya adalah untuk pemenuhan pengetahuan dan keterampilan dalam kinerja pada suatu pekerjaan dalam sebuah organisasi. Seperti yang telah diungkapkan "*Training strives to produce relevant and needed security skills and competencies*. Di dalam prgram training ini sudah terdapat kurikulum yang jelas dan ada tingkatan serta sertifikat.
c. *Education*, diungkapkan bahwa "*Education integrates all of security skills and competencies of the various functional specialties into common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialist and professionals capable of vision and pro-active response*". Contohnya dalah program degree pada perguruan tinggi atau universitas.
d. *Professional Development*, dilakukan untuk membangun profesional dalam karir security. Beberapa contohnya adalah IT *security officer*, IT *security auditor*, IT *contractor, system administrator,* dan sebagainya. Biasanya untuk program ini dilakukan sertifikasi yang fokus pada bidang tertentu.

Adapun tingkatan Program Pembelajaran Kemanan Siber dapat diketahui Gambar 4 berikut.



Gambar 4. IT Security Learning Continuum
Sumber : NISP SP 800-50 (NIST, 2003)

Program *security awareness* atau kesadaran keamanan merupakan tingkat dasar dalam mempelajari keamanan siber. Program ini yang paling sederhana untuk diterapkan. Karena program *awareness* tidak terlalu formal dan dapat dilakukan melalui media yang sangat beragam. Selain itu, program kesadaran keamanan juga lebih praktis karena materinya sederhana dan lebih menyentuh langsung pada hal-hal yang dibutuhkan oleh masyarakat dalam sehari-hari. Sehingga diharapkan dapat langsung diterapkan oleh masyarakat termasuk pada pelaku *e-commerce*.

Program kesadaran keamanan informasi diharapkan dapat langsung diterima dan dirasakan oleh masyarakat termasuk para konsumen *e-commerce* yang ada di Indonesia. Selain itu program awreness diharpapkan juga mampu menjangkau masyarakat secara luas dan mudah diphami dan diterapkan dalam kegiatan sehari hari termasuk dalam melakukan transaksi belanja di *e-commerce*.

Desain Program Keamanan Siber

Untuk menyukseskan kesadaran keamanan pada konsumen *e-commerce* perlu dibuat desain yang yang menggambarkan struktur dari program kesadaran keaaman siber, penilain kebutuhan, menyusun rencana program, penentuan prioritas, cara penyajian serta pertimbangan biaya yang diperlukan.

Mengingat para konsumen *e-commerce* tersebar di berbagai wilayah geografis di seluruh Indonesia, maka diperlukan upaya yang cermat dalam menentukan model struktur program kesadaran keamanan siber ini. Berbagai pilihan program tersebut dapat diberikan secara sentralisasi di pusat maupun desentralisasi dengan diserahkan ke daerah. Namun demikian, dengan adanya perkembangan teknologi saat ini, maka pendidtribusian program dan materi tidak terlalu mengalami kendala. Sehingga pemilihan struktur dapat diseuaikan dengan kebutuhan dengan lebih mudah.

Sementara itu, selain struktur penentuan kebutuhan terhadap materi keamanan siber juga perlu diperhatikan. Untuk menentukan kebutuhan terhadap jenis keamanan yang diinginkan oleh konsumen, maka dapat dilakukan survey. Bentuk survey ini dapat berupa wawancara , kuesioner serta studi terkait tren dalam industri, akademis dan pemerintahan. Hasil dari survei terkait kebutuhan keamanan siber inilah yang dapat dijadikan sebagai acuan dalam menyusun program keamanan siber. Desain maupun konten yang akan disusun dapat disesuaikan dengan kebutuhan di lapangan.

Pengembangan program keamanan siber di kalangan konsumen *e-commerce* juga perlu mengacu pada kebijakan yang relevan. Selain itu juga perlu disesuaikan dengan kebutuhan konsumen agar materinya bersesuaian dengan yang diharapkan. Sehingga program yang dibuat sebagai upaya dalam membangun kesadaran keamanan siber dapat berjalan seirama dengan kebijakan yang terkait dan tidak terjadi pelanggaran dalam pelaksanannya.

Hal lain yang perlu diperhatikan dalam membangun kesadaran keamanan siber ini adalah dalam penentuan prioritas. Sebaiknya materi keamanan siber yang menjadi diutamakan adalah materi yang paling besar kesenjangan pemahamannya di kalangan konsumen *e-commerce*. Sebagai contoh pada saat marak kasus ancaman serangan *wanna cry*, maka perlu diprioritaskan untuk membuat program awareness dengan konten terkait *wanna cry*. Pada saat banyak sekali masyarakat yang memerlukan informasi tentang *phising*, maka sebaiknya disusun materi tentang *phising*.

Hal berikutnya yang tidak kalah penting dalam membangun program keamanan siber adalah dalam penyajian konten. Konten yang disajikan secara menarik akan membuka peluang besar untuk menarik target untuk turut serta dalam program keamanan siber. Sehingga model pembuatan infografis, permainan, poster, buletin maupun video grafis yang bagus akan

turut menyukseskan keberhasilan program ini. Karena penyajian jenis ini cenderung *eye catching* dan menarik perhatian karena tidak membosankan.

Dalam hal penyajian konten dalam program keamanan siber ini, juga perlu diperhatikan gaya belajar seseorang. Gaya belajar tersebut meliputi audio, visual dan kinestetik. Sehingga konten yang disajikan dengan mengakomodir gaya belajar masyarakat akan lebih baik hasilnya.

Sementara itu untuk pembiayan dalam membangun program awareness dapat disusun dan dialokasikan dengan sebaik-baiknya. Teknologi telah sangat membantu efektivitas dan efisiensi dari program awareness. Karena dengan teknologi konten dapat disusun dengan lebih mudah dan dapat didistribusikan dengan biaya yang murah.

Konten Kesadaran Keamanan Informasi

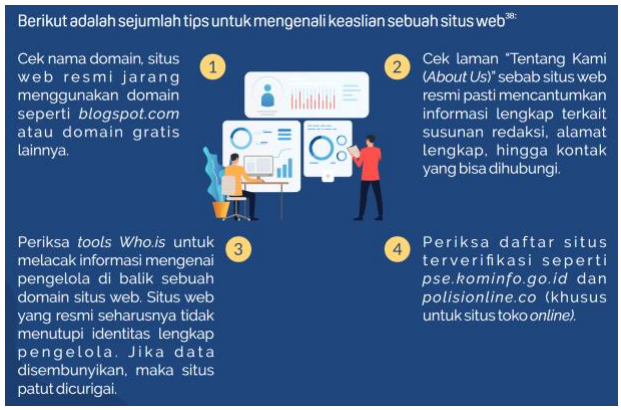
Dalam upaya membangun kesadaran keamaman siber ini pada *e-commerce* ini, konsumen perlu dibekali kewaspadaan terhadap ancaman siber saat akan melakukan transaksi di *e-commerce*. Beberapa jenis perilaku berikut ini dapat dijadikan konten pada program kesadaran keamanan siber:

a. Penggunaan password dan majemennya.
b. Cara melindungi dari serangan virus, worm, trojan horse, ransome ware, dan sebaginya.
c. Kebijakan terkait dengan keamanan siber
d. Perlakuan terhadap email masuk yang tidak dikenal.
e. Mengenal social engineering
f. Kemanan dasar dari perangkat
g. Cara membuat *back up* data
h. Dan sebagainya

Berbagai konten tersebut dapat disajikan agar masyarakat dapat mengenali, mengantisipasi dan mengetahui sikap yang harus diambil pada saat menemui ancaman siber tersebut. Selain itu penyajian juga dapat dibuat dalam berbagai format bentuk seperti narasi, gambar, maupun video yang menarik untuk disebarluaskan ke masyarakat. Metode lain untuk menyampaikan dapat dikemas dalam bentuk seminar, media sosial maupun grup organisasi.

Gambar 5 dan Gambar 6. berikut ini adalah contoh bentuk konten yang dikemas untuk dapat disebarluaskan dalam upaya membangun kesadaran keamanan siber. Gambar 5. merupakan salah satu contoh literasi digital untuk membangun kesadaran keamanan siber khususnya dalam mengenali keaslian situs web. Sedangkan gambar 6 merupakan contoh dalam mengenal *foot print* atau jejak digital.

Gambar 5: Tips mengenali situs website
Sumber: bssn.go.id



Gambar 6: *Digital foot print*
Sumber: bssn.go.id

Selain itu, agar upaya pembangunan kesadaran keamanan siber di kalangan konsumen ini dapat menjangkau masyarakat luas, maka konsumen yang telah mendapatkan pengetahuan tentang kesadaran keamanan siber ini dapat turut menyebarluaskan ke orang lain. Mereka diharapkan dapat mentransfer pengetahuannya ke masyarkat di lingkungannya baik membagikannya kepada , keluarga, dan orang yang terafiliasi dengannya. Sehingga di sini diperlukan kemapuan untuk berkomunikasi dengan baik.

KESIMPULAN

Ancaman dalam transaksi di e-commerce sangat berbahaya dan dapat menyerang para pelakunya termasuk konsumen. Oleh karena itu untuk melindunginya konsumen perlu dibekli dengan pehamanan tentang kesadaran keamanan siber. Dalam upaya membangun program keamann siber perlu diperhatikan pengaturan struktur, desain, konten, penyajian, penganggaran dan sebagainya. Dengan memperhatikan hal-hal tersebut diharapkan kegiatan pembangunan kesadaran keamanan siber di kalangan konsumen *e-commerce* ini dapat berhasil.

Selain itu agar upaya membangun keamanan siber pada konsumen *e-commerce* ini dapat berhasil disarankan untuk dapat didukung oleh penyedia market place untuk mengampanyekannya. Selain itu juga diperlukan kegiatan evaluasi secara terus menerus. Kegiatan evaluasi didasarkan pada data yang dapat diperoleh melalui wawancara, kuesioner, *focus discussion group* (FGD), dan lain-lain. Sehingga umpan balik yang didapatkan dapat digunakan untuk perbaikan program keamanan siber.

REFERENSI

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., Choudrie, J., Smith, K. J., Dhillon, G., Carter, L., Kortjan, N., Ramírez-Correa, P., Grandón, E. E., Alfaro-Pérez, J., Painén-Aravena, G., Chatchalermpun, S., Wuttidittachotti, P., Daengsi, T., Wang, X., Lee, K. M., Maynard Sean, B. (2020). A Cyber Security Awareness and Education Framework for South Africa. *Journal of Physics: Conference Series*, *51*(14), 103284. https://doi.org/10.1016/j.im.2020.103284%0Ahttps://doi.org/10.1016/j.tele.2020.101415%0Ahttps://doi.org/10.1016/j.ijinfomgt.2020.102123%0Ahttps://doi.org/10.1016/j.chb.2020.106531

Accurate online. (2018). https://penjualanresmiaccurate.id/bukti-bukti-indonesia-akan-menjadi-pasar-e-commerce-terbesar/

Bajaj, K. K. (2005). *E Commerce The Cutting Edge of Bussiness* (Second Edi). Tata Mac Graw Hill Publishing Company Limited. https://www.google.co.id/books/edition/E_Commerce/Co8iBAAAQBAJ?hl=id&gbpv=1&dq=cyber+awareness+and+e+commerce&pg=PP2&printsec=frontcover)

BPS. (2020). *Satistik E-commerce 2020*. BPS.

Desman, M. B. (2001). Building an Information Security Awareness Program. In *Building an Information Security Awareness Program* (Issue August 2014). https://doi.org/10.1201/9781420000054

Firdhy Esterina Christy. (2020). *Tempo*. https://data.tempo.co/read/909/prediksi-angka-pengguna-e-commerce-di-indonesia-2024

Irawan, aditya wicaksono, Yusufianto, A., Agustina, D., & Dean, R. (2020). Laporan Survei Internet APJII 2019 – 2020. *Asosiasi Penyelenggara Jasa Internet Indonesia*, *2020*, 1–146. https://apjii.or.id/survei

Khan, S. W. (2019). Cyber Security Issues and Challenges in E-Commerce. *SSRN Electronic Journal*, 1197–1204. https://doi.org/10.2139/ssrn.3323741

Kristian Angelo, a, Mary Jovy Anne, V., Azie Trina, M., & Jonathan, C. (2014). Privacy Awareness in E-Commerce. *International Journal of Education and Research*, *2*(1).

NIST. (2003). *NIST Special Publication 800-50*. U.S. Department of Commerce.

PCI Security Standards Council. (2014). Best Practices for Implementing a Security Awareness Program. *PCI Data Security Standard (PCI DSS)*, *October*, 12. https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Progr

am.pdf

Program, S. A. (n.d.). *Building an Effective and Comprehensive Security Awareness Program*.

Rahmadi, G., & Raf'ie Pratama, A. (2020). Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia. *Automata*, *1*(2). https://journal.uii.ac.id/AUTOMATA/article/view/15399

Reamer, F. G. (2018). Ethical Standards for Social Workers' Use of Technology: Emerging Consensus. *Journal of Social Work Values & Ethics*, *15*(2), 71–80.

Report, A. A. (2020). *Trust Services Security Incidents 2019*. *July*. https://doi.org/10.2824/277632

Teoh, C. S., & Mahmood, A. K. (2017). National cyber security strategies for digital economy. *International Conference on Research and Innovation in Information Systems, ICRIIS*, *July*. https://doi.org/10.1109/ICRIIS.2017.8002519

Widagdo, P. B. (2016). Perkembangan Electronic Commerce (E-Commerce) di Indonesia. *Researchgate.Net*, *December*, 1–10. https://www.researchgate.net/publication/311650384