BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi memberikan perubahan yang sangat signifikan terhadap strategi bisnis dunia usaha termasuk perbankan dengan menempatkan teknologi informasi sebagai unsur utama dalam proses produksi atau pemberian jasa. Selain itu perkembangan teknologi informasi juga telah mendorong inovasi di bidang jasa pelayanan termasuk jasa pelayanan perbankan. Pelayanan bank dalam bentuk internet banking sudah menjadi keharusan, karena kebutuhan dunia usaha dan nasabah bank semakin meningkat. Seiring dengan kemajuan teknologi maupun informasi, untuk itu internet banking dapat menjembatani kebutuhan dunia usaha maupun nasabah dalam hal mempercepat pelayanan jasa bank. (Maharsi, 2021).

Perkembangan dunia perbankan di Indonesia menjadi pusat perhatian masyarakat, dilihat dari persaingan kualitas produk, pelayanan jasa yang ditawarkan, dan melakukan promosi besar-besaran, sehingga perusahaan berlomba-lomba memberikan pelayanan terbaik dan memberikan kepuasan untuk menarik minat nasabahnya. Fungsi utama bank yaitu untuk menyimpan dana serta memberikan kemudahan dalam bertransaksi. Perbankan di Indonesia saat ini telah mengikuti perkembangan teknologi dan komunikasi sehingga mendorong terbentuknya *Mobile Banking* yang Merupakan layanan dari bank untuk melakukan transaksi yang dapat diakses memalui *online.* Fasilitas pada *Mobile Banking* meliputi transfer dana, informasi saldo, *mutase rekening*, pembayaran listrik, isi ulang pulsa, dan lainnya, yang membuat *Mobile Banking* menjadi penting dan sering kali digunakan dalam kegiatan sehari-hari. (Zulfahmi et al, 2023)

Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang diubah dengan Undang-Undang Nomor 19 Tahun 2016. Terkait aturan mengenai perlindungan terhadap transaksi digital, dimana setiap orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam teransaksi konsumen dalam teransaksi

elektronik sebagaimana dimaksud dalam pasal 28 ayat (1) dalam hal ini pemerintah memberikan dukung berdasarkan undang-undang tersebut dan mengawal terkait perkembangan ekonomi digital di Indonesia, termasuk *transformasi digitalisasi* perbankan. (Agustian et al, 2021)

Selain perundang - undangan tersebut di Indonesia sendiri pemerintah juga sudah mengeluarkan 60 Undang-undang yang mengatur ekonomi digital. di atas juga terdapat bahasan terkait keamanan sistem yang digunakan, maka dalam hal ini pemerintah membentuk tim *siber atau Badan Siber dan Sandi Negara (BSSN)* dalam perpres nomor 53 tahun 2017 Tentang Badan Siber dan Sandi Negara. dalam perpres tersebut disebutkan juga tugas BSSN pada pasal 2 yaitu melaksanakan tugas keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengkonsolidasikan semua unsur yang terkait dengan keamanan siber (Edy et al, 2022).

Meskipun telah ada undang – undang perlindungan transakisi digital perbankan namun tidak menjamin tidak akan ada kejahatan siber (*cyber crime*). seperti yang tertulis di (https://www.ojk.go.id/ojk-institute/id.) bahwa Sektor Perbankan paling banyak mengalami anomali internet. Anomali internet yang terjadi, mayoritas berasal dari serangan ransomware berdasarkan data pemantauan pada tahun 2023, di mana dari 160 juta anomali malware, sebanyak 966.533 terindikasi ransomware. pada tahun 2023, di mana skor indeks keamanan siber Indonesia sebesar 63,64 dari skala 100 atau meningkat sebesar 24,68 poin dibandingkan skor pada tahun 2022 yang hanya sebesar 38,96 poin. Skor ini menempatkan Indonesia pada peringkat 49 dari 176 negara pada tahun 2023, meningkat signifikan dibandingkan pada tahun 2022 yang hanya menduduki peringkat 83 dari 160 negara. Lalu Industri keuangan di wilayah Indonesia (hampir 50%) mengalami serangan *cyber crime* pada aplikasi *web dan API* selama 18 bulan terakhir dari Januari 2022 hingga Juni 2023. kerugian yang terjadi setara dengan 3,7 miliar dari total 7,4 miliar, meningkat sekitar 36% dari tahun ke tahun jika membandingkan kuartal II-2022 dengan kuartal III-2023. *cybercrime* atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (*network*) bahkan *cybercrime* dapat didefinisikan sebagai Pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal secara sengaja

yang menyebabkan reputasi korban tidak baik atau menyebabkan kerugian pada korban baik fisik maupun mental, baik secara langsung maupun tidak langsung yang menggunakan jaringan telekomunikasi moderen seperti, *Chat, email, notice boards*.

Menurut Alcianno (2019) dalam mengatasi serangan *cybercrime,* bank dapat mencapai keberhasilan dengan mengaitkan *technical skill* pada karyawan. Peningkatan keterampilan teknis menjadi kuci utama dalam membangun pertahanan keamanan siber yang efektif. Melalui pelatihan *sertifikasi Certified information system security profesional (CISSP)* Atau *certified ethical hacker (CEH*) dan pengembangan berkelanjutan, karyawan bank diberdayakan dengan (1) pengetahuan mendalam tentang keamanan siber, (2) termasuk identifikasi serangan, (3) pencegahan, dan (4) respons yang cepat. Point-point inilah yang menjadi dimensi untuk mengukur *technical skill* kali ini. Bank dapat membentuk tim keamanan internal yang terdiri dari individu dengan *technical skill* yang kuat, memastikan bahwa pemantauan aktivitas mencurigakan dan penanganan insiden dapat dilakukan secara efektif. Implementasi sistem keamanan yang terkini dan berkualitas tinggi menjadi landasan dalam melindungi aset digital.

Lalu untuk melalui simulasi serangan berkala, karyawan dapat menguji ketahanan sistem dan meningkatkan kemampuan respons terhadap situasi kritis. selain itu, bank dapat mendorong partisipasi karyawan dalam komunitas keamanan siber, memfasilitasi pembelajaran dan kolaborasi dengan para ahli industri. Program kesadaran keamanan rutin menjadi tambahan yang penting untuk meningkatkan pemahaman karyawan tentang ancaman siber, termasuk cara mengidentifikasi *phishing* dan melaporkan aktivitas mencurigakan. dengan cara ini, bank dapat menghadapi tantangan *cybercrime* dengan langkah-langkah yang proaktif dan mendalam, menciptakan lingkungan keamanan yang kuat dan responsif. (Riyanti, 2021)

Menurut UU No. 27 Tahun 2022 mengenai perlindungan data pribadi sepertinya tidak mampu mencegah serangan *Cybercrime* dan kebocoran data pribadi. hal ini terbukti dari maraknya serangan *Cybercrime* pada berbagai macam sektor industri baik perusahaan swasta maupun pemerintah. bahkan data BSSN menunjukkan bahwa pada tahun 2022, Indonesia mengalami sekitar 370 juta *cybercrime*. Data ini meningkat

cukup drastis dari tahun sebelumnya yakni 266 juta kasus sebagaimana yang dapat di lihat dalam grafik berikut ini:

Tabel 1. 1

Error Service Bank Syariah Indonesia (BSI)

Sumber : https://benaya.co.id.

Nurma et,al (2023), menjelaskan bahwa serangan *Cybercrime* juga terjadi pada layanan digital bank syariah indonesia (BSI) yang mengalami gangguan selama dua minggu. kasus peretasan yang diduga berupa serangan ransomware yang menyerang sistem digital atau teknologi BSI dan berdampak mengakibatkan dimana nasabah tidak dapat mengakses dan bertransaksi melalui Mbanking, mesin ATM, dan teller di kantor cabang bank. Lalu ada beberapa fitur pada aplikasi *mobile banking* ini bermasalah. aplikasi *Mobile banking* pada BSI tidak semuanya bisa digunakan semenjak adanya serangan *Ransomware*. Akan tetapi OJK menghimbau agar masyarakat tetap tenang dan berhati-hati dalam melakukan transaksi mewaspadai potensi penipuan maupun tindak kejahatan lainnya yang mengatas namakan suatu bank (https://ojk.go.id/id/berita).

Dengan maraknya serangan (*cybercrime)* didunia perbankan, dengan demikian diperlukan adanya *cybersecurity* yang merupakan sebuah upaya untuk memastikan bahwa atribut keamanan organisasi dan penggunaannya terjamin kemanannya. *cybersecurity* didefinisikan (Munawarah et al, 2021) sebagai praktik untuk melindungi sistem, jaringan, program, data dan informasi dari ancaman atau serangan digital. Berikut adalah beberapa elemen kunci dari keamanan siber menurut Munawarah (2022) yaitu : (1)Dokumen kebijakan privasi (*security policy);* (2) Infrastruktur

informasi *(Information infrastructure);* (3) Perimeter Pertahanan *(Perimeter Defense*); (4) Sistem pemantauan jaringan *(Network Monitoring System);* (5) Sistem Informasi dan Manajemen Peristiwa *(system Information and Event Management);* (6) Peringkat keamanan siber (*Network Security Assessment);* (7) Kesadaran sumber daya manusia dan keamanan (*Human resource and security awareness).*

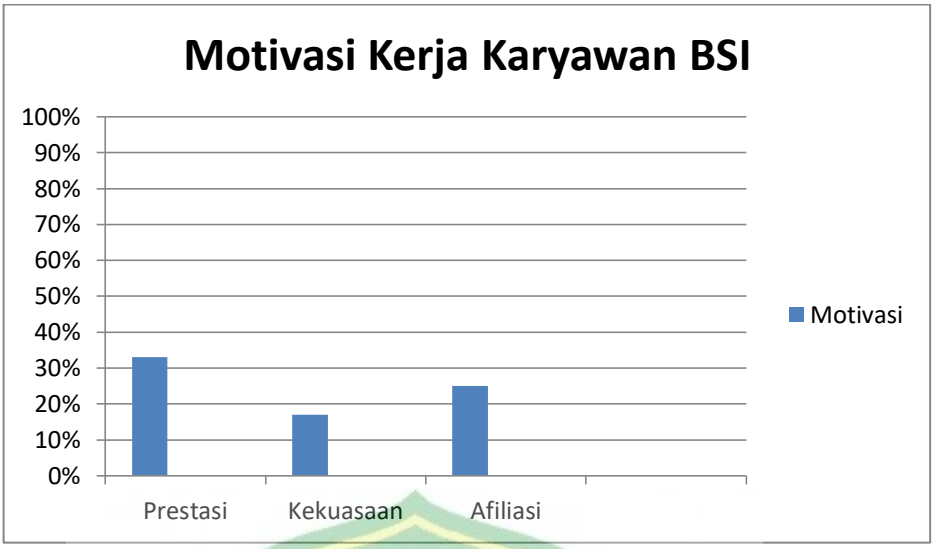
Menurut Menteri BUMN Erick Thohir terkait gangguan layanan perbankan di ATM maupun mobile banking BSI Pada Rabu 5 mei 2023 di Labuan bajo, menjelaskan bahwa bank BSI harus memperkuat sistem IT diinternal mereka. dalam hal ini berkaitan dengan *technical skill* karyawan untuk menjalakan tugas - tugas tertentu. kemampuan teknis ini dapat membantu setiap orang untuk menjadi lebih produktif dan efektif dalam melaksanakan pekerjaanya. kemampuan ini meliputi pengetahuan dan keterampilan dalam penggunaan alat dan teknologi yang relevan dalam bidang tersebut, termasuk mengelola jaringan internet dikantor. (https://kemenkeu.go.id)

Technical Skill pada dasarnya adalah kemampuan teknis yang diperlukan untuk menjalankan tugas-tugas tertentu. keterampilan berhubungan dengan kemampuan seseorang untuk melakukan atau menyelesaikan pekerjaan teknis seperti keterampilan manajemen TI. keterampilan atau keahlian *(skill)* yang dimiliki seorang pegawai untuk melaksanakan dan menyelesaikan tugas pekerjaannya. (Djien, 2021)

Adapun faktor pendukung kinerja karyawan yaitu kemampuan karena kemampuan kerja merupakan keahlian yang dimiliki karyawan dalam melakukan suatu pekerjaannya. Apabila bakat yang dimiliki karyawan dikembangkan dan digunakan dengan tepat maka dapat mempengaruhi perkembangan perusahaan (Arini, 2020), Selain kemampuan terdapat motivasi dan semangat kerja yang merupakan alat untuk menyalurkan dan mendukung perilaku karyawan untuk berkerja lebih giat dan semangat untuk mencapai hasil yang optimal (Tsauri, 2021)

Tabel 1. 2

Motivasi Kerja Karyawan BSI



Sumber : BSI Jatibarang

Dapat dilihat dari diagram 1.2 diatas yang didapatkan oleh peneliti dari hasil observasi yang dilakukan di BSI KCP Jatibarang Pada hari sabtu 11 Mei 2023 dengan beberapa karyawan memperoleh hasil, karyawan lebih termotivasi oleh pencapaian pribadi dan standar kinerja yang tinggi daripada

kebutuhan untuk diterima oleh rekan kerja atau untuk memegang posisi pengaruh dan kontrol. Mereka lebih berfokus pada pencapaian tujuan dan keberhasilan dalam tugas-tugas yang menantang. Hal ini biasanya membawa kepada produktivitas yang lebih tinggi, inovasi, dan kontribusi signifikan terhadap kemajuan organisasi. Akan tetapi, pada kenyataanyan kekuasaan merupakan pengaruh terbesar karena Dalam beberapa lingkungan kerja, struktur kekuasaan sangat menentukan siapa yang berhasil dan siapa yang tidak.untuk mendapatkan pengakuan, promosi, atau kesempatan. Data tersebut diperoleh melalui observasi dengan pembagian Google from yang isinya berkaitan dengan pernyataan indikator yaitu, Kebutuhan akan berprestasi, kebutuhan akan kekuasaan dan kebutuhan untuk berafiliasi. Dimana hasil dari masing-masing indikator tersebut memperoleh hasil kebutuhan akan prestasi sebesar 30%, kebutuhan akan kekuasaan sebesar 10%, dan kebutuhan akan berafiliasi sebesar 20%.

Seiring dengan itu karyawan yang memiliki keterampilan teknis yang tinggi bisa memperkuat sistem internal karyawan bank BSI agar bisa bersaing didunia digital, manajemen yang efektif terhadap *cybersecurity* akan melibatkan perencanaan proaktif,

penerapan kebijakan keamanan yang ketat, dan pelatihan terus-menerus kelancaran operasional yang berkelanjutan menjadi hasil alamiah dari kombinasi ini. dengan keterampilan teknis yang ditingkatkan, karyawan dapat beradaptasi dengan perubahan teknologi dengan lebih baik dan merespons secara efisien terhadap serangan saiber. Manajemen yang efektif menciptakan kerangka kerja yang kokoh untuk menjaga kelancaran operasional, meminimalkan risiko gangguan, dan mengoptimalkan ketrampilan teknis. (Hasibuan, 2020)

Menurut penelitian yang dilakukan Refi Halensi (2023) menjelaskan terkait *Technical skill* memberi pengaruh yang signifikan terhadap kinerja Karyawan, penelitian ini sejalan dengan Tengku Fachrozi (2023) dan Arsari Primadanti (2017). Kemudian pengembangan kualitas *Technical skill* Karyawan yang terkait *Cybersecurity* dapat dilakukan melalui pelatihan-pelatihan. Sedangkan menurut Machlul Alamin et.al (2023) menjelaskan dalam penelitiannya terkait peningkatan pemahaman *Cybersecurity* bahwa kegiatan pelatihan membantu meningkatkan pengetahuan dan keahlian terkait *Cybersecurity*, penelitian ini sejalan dengan Antika Zahratul Kamalia et.al (2024) dan Yusuf Indra Wijaya (2023).

Berdasarkan uraian di atas bahwa apabila ingin mencapai hasil yang maksimal Seorang karyawan harus bekerja dengan sungguh-sungguh dengan memberikan kemampuan yang dimiliki serta ditunjang oleh sarana dan prasarana yang ada. dimana kemampuan seseorang bisa di ukur dari tingkat manajemen keterampilan TI atau keahlian *(skill)* dan pengetahuan yang dimiliki dalam melaksanakan tugas yang telah diberikan.

Berdasarkan uraian latar belakang tersebut, penulis tertarik untuk melakukan penelitian lebih lanjut terkait dampak *cybersecurity* terhadap sektor perbankan, dengan fokus pada bagaimana tingkat keterampilan teknis karyawan bank syariah indonesia (BSI) yang dapat mempengaruhi motivasi kerja karyawan. yang berjudul **"PENGARUH *CYBERSECURITY* DAN *TECHNICAL SKILL* TERHADAP MOTIVASI KERJA KARYAWAN BSI WILAYAH INDRAMAYU "**

B. Perumusan Masalah

a. Identifikasi Masalah

Identifikasi yang dapat diambil dari latar belakang masalah diatas adalah sebagai berikut :

1. Maraknya serangan *cybercrime* terhadap dunia perbankan, membuka celah kejahatan *cybercrime*, seperti pencurian data nasabah dan pembobolan rekening.
2. Menurut data BSSN menunjukan pada tahun 2022 indonesia mengalami sekitar 370 juta serangan *cybercrime*
3. Kejahatan *cybercrime* juga terjadi pada layanan digital bank BSI yang mengalami gangguan selama dua minggu kasus ini diduga berupa *ransomware* dibeberapa fitur aplikasi *mobile banking*.
4. Menurut Eric tohir Bank BSI harus memperkuat sistem IT diinternal mereka yang berkaitan dengan *technical skill* karyawan.
5. Pengaruh serangan *cybercrime* terhadap kinerja karyawan bank BSI yang memberikan dampak negatif pada kinerja karyawan membuat karyawan sedikit tidak percaya diri saat menghadapi konsumen yang komplain.

b. Batasan masalah

Untuk menghindari kesalah pahaman dalam penelitian ini, peneliti membatasi masalah bahwa penelitian ini:

- Dilakukan di bank syariah indonesia KCP Jatibarang Indramayu.
- Penelitian ini hanya berfokus pada pengaruh *cybersecurity* dan *technical skill* terhadap motivasi kerja karyawan BSI Jatibarang.

c. Rumusan masalah

Masalah yang dapat dirumuskan dari identofikasi masalah dan batasan masalah diatas adalah sebagai berikut :

1. Bagaimana pengaruh *cybersecurity* terhadap motivasi kerja karyawan BSI wilayah indramayu ?
2. Bagaimana pengaruh technical skill terhadap motivasi kerja karyawan BSI wilayah indramayu?
3. Bagaimana pengaruh simultan antara *cybersecurity* dan *technical skill* terhadap motivasi kerja karyawan BSI wilayah indramayu?

C. Tujuan Penelitian

Berdasarkan rumusan masalah tersebut, tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Untuk menganalisis pengaruh *cybersecurity* terhadap motivasi kerja karyawan BSI wilayah indramayu.
2. Untuk menganalisis pengaruh *technical skill* terhadap motivasi kerja karyawan BSI wilayah indramayu.
3. Untuk menganalisis pengaruh simultan antara *cybersecurity* dan *technical skill* terhadap motivasi kerja karyawan BSI wilayah indramayu.

D. Manfaat Penelitian

Adapun kegunaan dari penelitian ini adalah sebagai berikut :

a. Manfaat Penulis

Penelitian ini dapat memberikan banyak maanfat kepada penulis sehingga penulis lebih memahami dan mengetahui terkait serangan *cybersecurity* dan *technical Skill* terhadap motivasi kerja karyawan bank syariah indonesia.

b. Manfaat Akademis

Hasil penelitian ini diharapkan dapat menjadi sumber informasi dan Pengetahuan mengenai gambaran tentang adanya serangan *cybersecurity* dan *technical skill* terhadap motivasi kerja karyawan bank syariah indonesia.

c. Manfaat Teoritis

Diharapkan penelitian ini dapat menjadi sumber informasi dan rujukan bagi peneliti selanjutnya sebagai salah satu gambaran tentang Pengaruh serangan *cybersecurity* dan *technical skill* terhadap motivasi kerja karyawan bank syariah indonesia.

E. Sistematika Penelitian

Dalam penyusunan skripsi ini, penulis membagi menjadi lima bab, adapun penelasan dari tiap-tiap bab sebagai berikut:

BAB 1 : PENDAHULUAN

Bab ini berisi tentang gambaran umum dari pembahasan yang meliputi : latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab ini berisi tentang landasan teori yang memuat tentang berbagai teori-teori, yakni teori *Cybersecurity*, *Technical skill,* dan motivasi kerja karyawan. Dalam bab ini juga terdapat kerangka berpikir, tinjauan pustaka yang dijadikan acuan dan pembeda antara penelitian ini dengan penelitian terdahulu. Dalam bab ini juga terdapat penyusunan hipotesis awal sebagai dugaan sementara dari penelitian ini.

BAB III : METODE PENELITIAN

Pada bab ini berisi tentang metode penelitian, pendekatan dan jenis penelitian, lokasi dan objek penelitian, populasi dan sampel penelitian, jenis dan sumber data, metode pengumpulan data, teknik pengelolaan dan analisa data yang digunakan oprasional variabel dan uji instrumen.

BAB IV : HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menjelaskan deskripsi objek penelitian dan hasil analisis serta pembahasan secara mendalam tentang hasil penelitian. Hasil penelitian memuat data utama, data penunjang, dan pelengkap yang diperlukan di dalam penelitian ini.

BAB V : PENUTUP

Bab ini adalah penutup yang terdiri dari dua sub bab yaitu kesimpulan dari hasil peneliti dan saran yang membangun untuk objek penelitian.