El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam

Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Analisis Manajemen Risiko Keamanan *Self-Service Technology* Perbankan Syariah

Neli Nurzaqiah[1*)], MH Ainulyaqin[2)], LI Achmad[3)], Sarwo Edy[4)]
[1, 2, 3, 4,] Fakultas Agama Islam, Universitas Pelita Bangsa
Korespondensi: nelinz472@gmail.com

ABSTRACT

Self Service Technology (SST) is a technology that allows customers to make transactions or carry out services independently without depending on employees. In the banking world, the Self-Service Technology services that customers can use are Automatic Teller Machine (ATM), Mobile Banking and Internet banking services to make things easier customers. However, you must be aware of various risks or potential incidents that could occur when customers use SST services. This research aims to analyze the security risk management of Sharia Banking Self-Service Technology. This research method uses a qualitative approach with field study methods through interviews and documentation. The results of this research are that Bank BJB Syariah has implemented Self-Service Technology security risk management with various strategies to minimize the security risks of Sharia Banking Self-Service Technology.

Keywords: *Self Service Technology, Sharia Banking, Automatic Teller Machine, Mobile Banking, Internet Banking*

ABSTRAK

Self Service Technology (SST) merupakan teknologi yang memungkinkan nasabah untuk bertransaksi ataupun melakukan pelayanan secara mandiri tanpa tergantung pada karyawan, pada dunia perbankan layanan *Self Service Technology* yang dapat digunakan nasabah yaitu layanan *Automatic Teller Machine (ATM), Mobile Banking dan Internet banking* guna mempermudah nasabah. Namun dengan begitu harus diwaspadai dengan berbagai risiko atau potensi kejadian yang dapat terjadi ketika nasabah menggunakan layanan SST. Penelitian ini bertujuan untuk menganalisis manajemen risiko keamanan *Self-Service Technology* Perbankan Syariah. Metode penelitian ini menggunakan pendekatan kualitatif dengan metode studi lapangan melalui wawancara dan dokumentasi. Adapun hasil dari penelitian ini adalah Bank BJB Syariah telah menjalankan manajemen risiko keamanan *Self-Service Technology* dengan berbagai strategi untuk meminimalisir risiko-risiko keamanan Self-Service Technology Perbankan Syariah.

Kata kunci: *Self Service Technology*, Perbankan Syariah, *Automatic Teller Machine, Mobile Banking, Internet Banking*

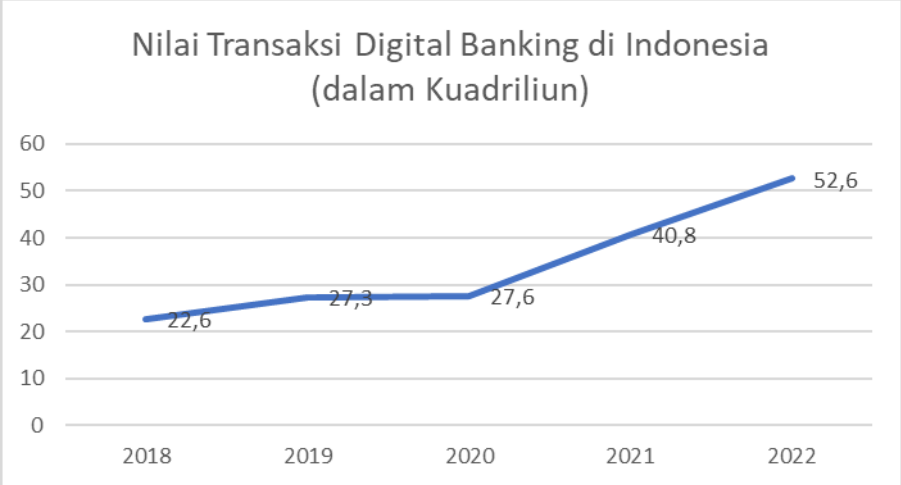
PENDAHULUAN

Di era digital saat ini, teknologi merupakan salah satu sarana yang dapat digunakan untuk memaksimalkan kinerja perusahaan atau entitas tertentu khususnya industri perbankan. Dengan semakin pesatnya perkembangan teknologi, maka akan memberikan dampak yang luar biasa pada semua aspek kehidupan

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

manusia. Teknologi informasi berbasis sistem khususnya perkembangan internet telah memberikan dampak yang sangat pesat terhadap proses bisnis industri perbankan. Industri perbankan sendiri merupakan sektor industri yang sangat besar dalam penggunaan teknologi informasi. Oleh karena itu, penerapan teknologi informasi bank akan mendorong kegiatan operasionalnya dan meningkatkan pelayanan kepada nasabah dan masyarakat. Semakin meningkatnya penggunaan perangkat *mobile* dan komputer sebagai media transaksi keuangan, maka peran teknologi informasi menjadi aspek yang sangat penting. Hal ini juga disebabkan oleh meningkatnya penggunaan Internet di Indonesia yang diikuti dengan perluasan pembangunan infrastruktur jaringan Internet (Arnita, dkk, 2023).

Industri perbankan syariah mengalami pertumbuhan yang pesat dan mampu mendorong kegiatan ekonomi. Hal tersebut dapat dikatakan karena perbankan syariah telah menjadi salah satu industri yang dapat membantu mendistribusikan dana publik dengan cara yang paling produktif bagi perekonomian, serta juga berfungsi sebagai perantara yang dapat membantu memperlancar aliran uang antara berbagai lembaga dengan sektor ekonomi lainnya. Meskipun dari segi keberadaan dan peranan bank syariah telah mengalami perkembangan yang begitu pesat, yang ditandai dengan banyaknya berdirinya bank-bank syariah. Namun perkembangan teknologi pada saat ini telah mempengaruhi perubahan sosial di tengah-tengah masyarakat. Pengaruh teknologi menjadikan seseorang sangat memiliki ketergantungan atas keberadaannya. Munculnya teknologi lebih memudahkan masyarakat dalam mendapatkan informasi. Sehingga dapat dikatakan bahwa media sosial merupakan perpaduan antara sosiologi dan teknologi (Tartila, 2022).



Gambar 1. Grafik Transaksi *Digital Banking* di Indonesia

Berdasarkan grafik di atas, nilai transaksi *digital banking* di Indonesia naik dari tahun ke tahunnya (*year-on-year*/yoy). Pada tahun 2018 nilai transaksi *digital banking* di Indonesia senilai 22,6 kuadriliun, jumlahnya terus meningkat hingga mencapai tingkat tertinggi pada tahun 2022 dimana transaksi *digital banking* di Indonesia mencapai 52,66 kuadriliun. Menurut Kepala Departemen Komunikasi BI

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Erwin Haryono dalam siaran persnya "Transaksi sistem pembayaran terus naik dengan stabilitas sistem yang terjaga dan layanan pembayaran digital yang semakin meningkat" (Ahdiat, 2023).

Teknologi di bidang perbankan dimanfaatkan dalam proses promosi, pemasaran, sampai dengan alat bantu transaksi yang berbasis teknologi. Pengusaha di bidang perbankan telah bekerja keras untuk saling bersaing dalam pengembangan produk layanan mereka yang berbasis teknologi. Layanan yang diberikan oleh pihak perbankan dalam memanfaatkan teknologi sering disebut dengan istilah *digital banking*, yang mana di dalamnya mencakup layanan seperti *Automatic Teller Machine* (ATM) yaitu sebuah alat elektronik yang mengizinkan nasabah bank untuk mengambil uang dan mengecek rekening tabungan mereka tanpa perlu dilayani oleh seorang *teller* atau kasir (Rochmah and Ernawati, 2022). ATM memberikan kemudahan kepada nasabah dalam melakukan transaksi perbankan secara otomatis melalui mesin ATM dan untuk melakukan berbagai jenis pembelian atau pembayaran tagihan tanpa harus datang ke kantor cabang dan tanpa terikat waktu (Azizah dkk).

Selain itu juga perbankan memberikan layanan *Mobile Banking* dengan tujuan memberikan kemudahan bagi nasabah untuk melakukan transaksi finansial seperti mentransfer uang baik sesama jenis bank maupun antar bank *online*, pembayaran zakat, wakaf uang, BPJS serta pembelian token maupun pulsa (Andrian dkk, 2023). Jadi *Mobile Banking* ini diharapkan benar-benar dapat membantu nasabah dengan memberikan kemudahan dan kenyamanan dalam bertransaksi. Perbankan juga memberikan layanan *Internet Banking*, yaitu layanan bank yang memanfaatkan kecerdasan teknologi dimana para nasabah bisa melakukan transaksi secara *mobile* berbasis internet, dengan tujuan memudahkan proses transaksi, perolehan dana dengan cara yang mudah dan cepat, dan pemrosesan pembayaran di cara yang cepat dan nyaman (Leviani & Wiyono, 2023). Ketiga fasilitas tersebut sering disebut dengan istilah *Self Service Technology* (SST). Jadi sudah tampak jelas digitalisasi perbankan dapat mengurangi aktivitas nasabah di kantor cabang, walaupun memang tidak bisa menggantikan keberadaan kantor cabang itu sendiri. Tetapi tidak bisa dipungkiri masih ada nasabah-nasabah yang belum siap menerima digitalisasi dan masih nyaman dengan layanan perbankan langsung, serta transaksi-transaksi bernilai besar yang masih harus dilakukan secara fisik. Bank digital pun hadir dan akan lebih fokus melayani transaksi individual dan ritel (Yolandha, 2021).

Fasilitas SST pada perbankan sangat dibutuhkan oleh Masyarakat dalam melakukan transaksi dengan mudah yang biasanya berhubungan dengan pemenuhan keinginan mereka. Semakin baik pelayanan yang diberikan pada fasilitas SST tersebut maka akan sangat berpengaruh terhadap perilaku dan kepuasan yang dihasilkan oleh nasabah. Layanan *Self Service Technology* memang diciptakan agar nasabah dapat lebih mudah melakukan transaksi perbankan. Tetapi nasabah tetap harus berhati-hati karena layanan perbankan ini rentan akan risiko. Disamping adanya kemungkinan risiko yang disebabkan oleh operasional bank maupun kelalaian

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

nasabah, adapun risiko yang sering dialami pada layanan *E-banking*, seperti halnya pada *mobile banking*, yaitu *cyber crime* (Suhaemin & Muslih, 2023).

Menurut Wareza (2021) bahwa *Automatic Teller Machine* (ATM), *Mobile Banking* dan *Internet Banking* telah banyak digunakan di era teknologi pada saat ini, kemudian faktor keamanan dan risiko sangatlah mempengaruhi masyarakat dalam penggunaan *digital banking*. Apalagi dengan berkembangnya teknologi yang semakin maju telah memudahkan masyarakat untuk bertransaksi. Jenis serangan yang baru-baru ini terjadi di Indonesia bahkan memungkinkan *hacker* untuk meninggalkan jejak di sistem perbankan dan menguncinya. Para *hacker* ini nantinya akan meminta tebusan kepada perbankan untuk bisa mengakses kembali sistemnya ini. Tantangan selanjutnya adalah keamanan data nasabah, baik mengenai data yang disampaikan nasabah kepada perbankan hingga data transaksi nasabah. Selain itu manajemen risiko dari penggunaan teknologi di sistem perbankan adalah adanya risiko kebocoran data hingga penggunaan *outsourcing* untuk penyimpanan data nasabah.

Gambar 2. Grafik Kasus Kebocoran Data di Indonesia

Berdasarkan grafik tersebut, masih banyak data-data yang mengalami kebocoran, dapat dilihat pada tahun 2020 kebocoran itu mencapai tingkat tertinggi sebanyak 14,37 juta akun. Tetapi jumlah akun yang mengalami kebocoran data di Indonesia mengalami penurunan sebanyak 13 juta menjadi 1,03 juta pada tahun 2021, dan terus mengalami penurunan hingga tahun 2022. Hal itu menandakan bahwa tingkat keamanan untuk mengantisipasi kebocoran data-data di Indonesia sudah mulai membaik dalam dua tahun terakhir dengan rata-rata 0,93 juta (Dihni, 2022).

Terdapat kasus-kasus kebocoran yang terjadi pada dunia perbankan di Indonesia, seperti yang diberitakan oleh Natalia dalam CNBC Indonesia, Bank Syariah Indonesia (BRIS) sempat kena serangan siber karena sejak 8 Mei 2023 layanan ATM

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

dan *m-banking* tidak dapat digunakan, hingga lebih dari sepekan layanan keuangan masih sulit diakses dan membuat nasabah khawatir. Sistem layanan BSI diketahui terkena serangan *ransomware* oleh kelompok *Lockbit* (Natalia, 2023). Pada Oktober 2021, beredar informasi *database* Bank Jatim (BJTM) bocor. Dilansir Antara, *database* Bank Jatim dijual di forum pengumpul data hasil kebocoran *database* RaidForums. *Database* tersebut dijual dengan harga US$250.000 sebesar 378 GB yang berisi data seperti data nasabah, data karyawan, data keuangan pribadi, dan lainnya (Rini, 2023). Pada Januari 2022, Bank Indonesia (BI) menjadi korban serangan *ransomware* jenis Conti ke dalam jaringan BI. Insiden kala itu menimpa kantor BI di Bengkulu yang menyebabkan kebocoran data. Juru Bicara Badan Siber dan Sandi Negara (BSSN) Anton Setiawan mengungkapkan, pelaku menyerang 16 perangkat komputer personal di kantor tersebut. Pihak BI dan BSSN pun langsung membentuk tim untuk mitigasi (Pratama, 2023). Bank umum di Indonesia tercatat mengalami kerugian riil sebesar Rp246,5 miliar akibat serangan siber yang melanda industri perbankan sepanjang semester I/202 dengan *potential loss* Rp208,4 miliar, sementara nilai pemulihan Rp302,5 miliar. Adapun kerugian riil yang dialami pihak lain sebesar Rp9,1 miliar dan *potential loss* mencapai Rp3,8 miliar, nilai *recovery* Rp3,8 miliar (Damara, 2021).

Penelitian yang dilakukan oleh Abdul Malik Fajri dan Evony Silvino Violita (2023) dengan judul Analisis Manajemen Risiko Bank Syariah Dalam Melakukan Transformasi Digital (Studi Kasus Pada Bank A S), hasil penelitian menunjukkan bahwa Bank AS sudah mempunyai implementasi risiko manajemen terkait teknologi informasi dalam melakukan transformasi digital yang ada sejalan dengan ketiga komponen *Risk IT Framework*. Penelitian Khabib Solihin dan Fajar Adhi Kurniawan (2022) dengan judul Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam menghadapi ancaman *Cyber Security*, dari hasil penelitian menunjukkan bahwa penerapan manajemen risiko di KSPPS Artha Bahana Syariah terkait dengan ancaman *cyber security* dalam bentuk pengawasan aktif oleh pimpinan, kecukupan kebijakan dan prosedur penggunaan teknologi informasi, kecukupan proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko teknologi informasi, dan sistem pengendalian internal atas penggunaan teknologi informasi. Sedangkan penelitian Muhazzab Alief Faizal dkk (2023) dengan judul Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman dan Tantangan Terkini dengan kesimpulan, menghadapi ancaman terkini terkait risiko teknologi informasi pada bank syariah memerlukan implementasi sistem keamanan yang tepat. Dengan identifikasi dan evaluasi risiko yang komprehensif, penggunaan teknologi keamanan yang mutakhir, pengawasan dan pemantauan yang aktif, serta pelatihan dan kesadaran keamanan yang terus menerus, bank syariah dapat mengurangi risiko serangan dan melindungi sistem perbankan mereka dengan lebih efektif. Implementasi kebijakan keamanan yang jelas, evaluasi dan pengujian keamanan teratur, serta pematuhan terhadap regulasi dan kebijakan privasi juga merupakan faktor penting dalam menjaga keamanan sistem.

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Penelitian-penelitian terdahulu telah banyak meneliti tentang manajemen risiko terkait teknologi informasi dalam melakukan transformasi digital dalam menghadapi Ancaman *Cyber Security* pada perbankan syariah. Adapun yang menjadi perbedaan penelitian ini dengan penelitian sebelumnya adalah penelitian ini lebih memfokuskan pada tingkat risiko keamanan *Self Service Technology* pada perbankan syariah. Berdasarkan uraian di atas, maka perlu dicermati lebih lanjut mengenai tingkat risiko keamanan layanan *automatic teller machine* (ATM), *mobile banking*, dan *internet banking* atau disebut dengan *Self Service Technology* perbankan syariah yang dapat dioperasikan secara mandiri tersebut.

METODE PENELITIAN

Lokasi yang dipilih dalam penelitian ini adalah Bank BJB Syariah KCP Lippo Cikarang yang berlokasi di Cikarang Central City, kabupaten Bekasi, Jawa Barat. Metode penelitian yang digunakan dalam penelitian ini adalah melalui pendekatan kualitatif dengan metode studi lapangan. Penelitian ini bersifat deskriptif yang bertujuan untuk menjelaskan mengenai strategi yang digunakan dalam memanajemen risiko serta cara penyelesaian dalam menghadapi risiko pada *Self-Service Technology* perbankan syariah tersebut. Teknik pengumpulan data yang dilakukan yaitu melalui wawancara, wawancara ini dilakukan dengan informan yaitu Bapak Puguh Setiawan, S.T selaku pimpinan KCP Bank BJB Syariah KCP Lippo Cikarang dan Bapak Muhammad Rizky Barnaz selaku *General Support Staff* Bank BJB Syariah KCP Lippo Cikarang. Didalam penelitian ini, peneliti melakukan observasi dengan terjun langsung ke Bank BJB Syariah KCP Lippo Cikarang. Observasi yang digunakan oleh peneliti yaitu observasi sistemastis, observasi sistematis adalah metode pengamatan yang dilakukan sesuai dengan prosedur atau ketentuan yang sudah dirancang sebelumnya. Selain itu peneliti melakukan dokumentasi, dokumen ini digunakan untuk mengetahui hasil wawancara yang berupa rekaman suara, catatan, dan foto.

HASIL DAN PEMBAHASAN

Hasil

Bank BJB Syariah merupakan bank yang memiliki tanggung jawab besar sebagai salah satu pelaku ekonomi Indonesia untuk memberikan pelayanan kepada masyarakat luas agar mereka menjadi sumber daya nasional yang tangguh dan terbaik, dengan memberikan edukasi/pendidikan perbankan yang baik, benar, dan sesuai dengan syariah. Namun, beberapa Bank BJB Syariah masih sulit ditemukannya fasilitas ATM yang tersebar di seluruh wilayah Indonesia. Dari segi ATM yang ada di bank syariah masih tertinggal jauh jika dibandingkan dengan bank konvensional, karena *Self-Service Technology* pada sektor perbankan telah digunakan pertama kali digunakan oleh perbankan konvensional, yang mana perbankan konvensional adalah perusahaan pertama yang dikenal oleh masyarakat. Maka dari itu, bahwa kualitas

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

layanan pada fasilitas *Self-Service Technology* di perbankan konvensional sudah tidak asing lagi ditelinga masyarakat. Hal ini dapat dijadikan sebagai kelemahan dari segi fasilitas *Self-Service Technology* di bank syariah dimata nasabah. Namun, itu semua bisa dijadikan motivasi sebagai umat Islam agar bisa berkontribusi dalam membantu perekonomian Islam melalui perbankan syariah.

Semakin berkembangnya zaman, maka perbankan syariah pun sudah mulai mengalami perkembangan yang cukup baik. Dan untuk pada saat ini di perbankan syariah pun sudah mempunyai fasilitas *Self-Service Technology* dan nasabah yang melakukan transaksi di bank syariah pun sudah semakin banyak. Meskipun perkembangan layanan perbankan digital begitu cepat, namun kemajuan ini juga harus diwaspadai dengan berbagai masalah dan risiko-risiko yang timbul. Berikut cara Bank BJB Syariah meminimalisir risiko keamanan *Automatic Teller Machine* (ATM) berdasarkan observasi di lapangan sebagai berikut:

1) Risiko perlindungan data pribadi

   Bank BJB Syariah memiliki tips untuk nasabah bagaimana cara mencegah terjadinya risiko keamanan risiko keamanan pada *Automatic Teller Machine* (ATM), yaitu untuk memastikan kepada nasabah untuk tidak memberikan kode OTP *(One Time Password).* Kode OTP tidak boleh diberikan kepada siapa pun karena berisi informasi rahasia.
2) Risiko Strategis Investasi di bidang IT

   Bank BJB Syariah memiliki cara untuk mengatasi risiko tersebut, yaitu dengan menerapkan penggunaan teknologi keamanan.
3) Risiko Serangan Siber

   Pada risiko ini, Bank BJB Syariah mengingatkan kepada nasabah bahwa penting bagi Masyarakat atau nasabah untuk bisa membuat user ID dan *password* cukup kompleks.
4) Risiko Kebocoran Data Nasabah

   Untuk mengatasi risiko tersebut, Bank BJB Syariah mengingatkan kepada nasabah untuk tidak memberikan kode verifikasi ATM karena kode tersebut bersifat rahasia dan hanya diketahui oleh pemilik kartu debit.

   Berikut cara Bank BJB Syariah meminimalisir risiko keamanan *Mobile Banking* berdasarkan observasi sebagai berikut:

1) Risiko Perlindungan Data Pribadi pada *Mobile Banking*

   Dalam mengatasi risiko tersebut, Bank BJB Syariah memberikan pendidikan dan kesadaran kepada nasabah untuk tidak membagikan informasi pribadi mereka.
2) Risiko Strategis Investasi di bidang IT

   Pada risiko ini, Bank BJB Syariah mengatasinya dengan cara melakukan langkah preventif penguatan sistem keamanan teknologi informasi.
3) Risiko Serangan Siber

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Dalam memanajemen kasus tersebut, Bank BJB Syariah menggunakan teknologi kriptografi yang aman dan terbaru, yang dapat membantu melindungi transaksi dan data nasabah

4) Risiko Kebocoran Data Nasabah

Cara mengatasi risiko tersebut, Bank BJB Syariah memantau sistem *Mobile Banking* secara teratur untuk memastikan bahwa tidak ada kelemahan keamanan yang dapat digunakan oleh pihak-pihak yang tidak berwenang.

Berikut cara Bank BJB Syariah meminimalisir risiko keamanan *Internet Banking* berdasarkan observasi sebagai berikut:

1) Risiko Perlindungan Data Pribadi

Dalam mengatasi risiko tersebut, Bank BJB Syariah memberikan edukasi dan kesadaran kepada nasabah untuk menjaga keamanan data pribadi dengan waspada saat menggunakan *wi-fi* publik.

2) Risiko Strategis Investasi di bidang IT

Dalam memanajemen risiko tersebut, Bank BJB Syariah menggunakan protokol koneksi yang aman.

3) Risiko Serangan Siber

Bank BJB Syariah memiliki cara untuk mengatasi risiko tersebut, yaitu dengan cara menggunakan antivirus yang efektif.

4) Risiko Kebocoran Data Nasabah

Dalam mengatasi risiko tersebut, Bank BJB Syariah memberikan pendidikan dan kesadaran kepada nasabah untuk berhati-hati dengan *link* atau situs palsu. Berhati-hati dengan *link* atau situs palsu sangat penting karena mereka dapat berisiko besar terhadap keamanan data pribadi dan keuangan (Hasil wawancara Bapak. Puguh Setiawan,S.T).

Pembahasan

Bank Syariah harus memiliki strategi dalam menangani risiko *pada Self-Service Technology* (SST) karena digitalisasi perbankan melalui SST telah meningkatkan transaksi digital dan memungkinkan nasabah untuk melakukan berbagai transaksi secara mandiri. Namun, ini juga meningkatkan risiko operasional, strategis, dan reputasi yang harus dihadapi oleh bank. Risiko operasional dapat timbul dari masalah teknis atau sistem yang mengganggu transaksi, sementara risiko strategis dapat berasal dari kegagalan bank dalam menyesuaikan diri dengan perkembangan teknologi dan kebutuhan nasabah. Risiko reputasi dapat timbul dari kegagalan bank dalam menjaga keamanan dan kerahasiaan transaksi nasabah. Untuk menghadapi risiko ini, bank syariah harus memiliki strategi yang efektif dalam mengelola dan mengurangi risiko yang terkait dengan SST. Berikut cara Bank BJB Syariah meminimalisir risiko keamanan *Self-Service Technology* berdasarkan observasi di lapangan sebagai berikut:

1) Cara Bank BJB Syariah meminimalisir risiko keamanan *Automatic Teller Machine* (ATM) berdasarkan observasi di lapangan sebagai berikut:

a) Risiko perlindungan data pribadi

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Bank BJB Syariah memiliki *tips* untuk nasabah bagaimana cara mencegah terjadinya risiko keamanan risiko keamanan pada *Automatic Teller Machine* (ATM), yaitu untuk memastikan kepada nasabah untuk tidak memberikan kode OTP *(One Time Password)*. Kode OTP tidak boleh diberikan kepada siapa pun karena berisi informasi rahasia yang sangat penting untuk mengamankan dan melakukan verifikasi akun. Jika kode OTP diketahui orang lain, mereka dapat menggunakan informasi tersebut untuk membobol akun digital, mencuri akun media sosial, merampas isi rekening bank, serta menyalahgunakan akun aplikasi Anda. Dengan demikian, memberikan kode OTP kepada siapa pun dapat berisiko besar terhadap keamanan data dan keamanan digital.

b) Risiko Strategis Investasi di bidang IT

Bank BJB Syariah memiliki cara untuk mengatasi risiko tersebut, yaitu dengan menerapkan penggunaan teknologi keamanan. Penggunaan teknologi keamanan yang canggih seperti sistem *cryptography*, yang berarti melakukan pengamanan komunikasi ataupun informasi menjadi kode rahasia sehingga menjadi aman dan dapat membantu dalam mengurangi risiko keamanan pada ATM. Sistem keamanan ini dapat meliputi penggunaan kartu plastik dan kode pengenal diri yang aman.

c) Risiko Serangan Siber

Pada risiko ini, Bank BJB Syariah mengingatkan kepada nasabah bahwa penting bagi Masyarakat atau nasabah untuk bisa membuat *user ID* dan *password* cukup kompleks. Karena itu relatif aman, sehingga tidak mudah ditebak oleh para *hacker*. Selain itu Bank BJB Syariah memberikan pendidikan dan kesadaran kepada nasabah tentang pentingnya keamanan dalam menggunakan ATM. Nasabah harus diingatkan untuk tidak membagikan informasi pribadi dan untuk selalu memantau aktivitas transaksi mereka. Bank BJB Syariah juga melakukan pencegahan lain seperti memberikan sosialisasi dan edukasi kepada nasabah tentang cara menggunakan ATM secara aman dan melakukan transaksi keuangan secara *online* dengan cara yang tepat.

d) Risiko Kebocoran Data Nasabah

Untuk mengatasi risiko tersebut, Bank BJB Syariah mengingatkan kepada nasabah untuk tidak memberikan kode verifikasi ATM karena kode tersebut bersifat rahasia dan hanya diketahui oleh pemilik kartu debit. Kode verifikasi ATM, berfungsi untuk mengamankan transaksi nasabah dan melindungi kartu debit dari penyalahgunaan. Jika kode tersebut diketahui oleh orang lain, maka mereka dapat melakukan transaksi ilegal menggunakan kartu debit, seperti penipuan transaksi atau pembobolan rekening. Oleh karena itu, sangat penting untuk menjaga kerahasiaan kode verifikasi ATM dan tidak memberikannya kepada siapa pun, termasuk kepada orang yang mengaku sebagai pihak bank

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

2) Cara Bank BJB Syariah meminimalisir risiko keamanan *Mobile Banking* berdasarkan observasi sebagai berikut:

a) Risiko Perlindungan Data Pribadi

Dalam mengatasi risiko tersebut, Bank BJB Syariah memberikan edukasi dan kesadaran kepada nasabah tentang pentingnya keamanan dalam menggunakan *Mobile Banking*. Nasabah harus diingatkan untuk tidak membagikan informasi pribadi dan untuk selalu memantau aktivitas transaksi mereka.

b) Risiko Strategis Investasi di bidang IT

Pada risiko ini, Bank BJB Syariah mengatasinya dengan cara melakukan langkah preventif penguatan sistem keamanan teknologi informasi terhadap potensi gangguan data dengan peningkatan proteksi dan ketahanan sistem.

c) Risiko Serangan Siber

Dalam memanajemen kasus tersebut, Bank BJB Syariah menggunakan teknologi *kriptografi* yang aman dan terbaru, yang dapat membantu melindungi transaksi dan data nasabah dengan cara mengenkripsi data sehingga hanya dapat diakses oleh pihak yang berwenang.

d) Risiko Kebocoran Data Nasabah

Cara mengatasi risiko tersebut, Bank BJB Syariah memantau sistem *Mobile Banking* secara teratur untuk memastikan bahwa tidak ada kelemahan keamanan yang dapat digunakan oleh pihak-pihak yang tidak berwenang.

3) Cara Bank BJB Syariah meminimalisir risiko keamanan *Internet Banking* berdasarkan observasi sebagai berikut:

a) Risiko Perlindungan Data Pribadi

Dalam mengatasi risiko tersebut, Bank BJB Syariah memberikan edukasi dan kesadaran kepada nasabah untuk menjaga keamanan data pribadi dengan waspada saat menggunakan *wi-fi* publik. Kita harus menjaga keamanan data pribadi dengan waspada saat menggunakan wi-fi publik karena penggunaan *wi-fi* publik dapat berisiko terkena pencurian data pribadi, kebocoran data pribadi, hingga jual beli data pribadi, yang dapat berbahaya bagi keamanan data pribadi.

b) Risiko Strategis Investasi di bidang IT

Dalam memanajemen risiko tersebut, Bank BJB Syariah menggunakan protokol koneksi yang aman seperti HTTPS dapat membantu melindungi data yang dikirimkan melalui *internet banking* dari *intercept* dan manipulasi .

c) Risiko Serangan Siber

Bank BJB Syariah memiliki cara untuk mengatasi risiko tersebut, yaitu dengan cara menggunakan antivirus yang efektif dapat membantu melindungi sistem *Internet Banking* dari serangan *cyber* dan virus.

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

d) Risiko Kebocoran Data Nasabah

Dalam mengatasi risiko tersebut, Bank BJB Syariah memberikan edukasi dan kesadaran kepada nasabah untuk berhati-hati dengan *link* atau situs palsu. Berhati-hati dengan atau situs palsu sangat penting karena mereka dapat berisiko besar terhadap keamanan data pribadi dan keuangan. Situs palsu biasanya dibuat untuk melakukan penipuan, pencurian identitas, atau menginfeksi komputer pengguna dengan *malware*. Mereka dapat meniru tampilan situs web asli dengan sangat akurat, sehingga pengguna sulit membedakan situs asli dengan situs palsu. Situs palsu dapat menawarkan tawaran yang tidak realistis, seperti hadiah besar, undian, atau diskon luar biasa, untuk menarik korban dan memikat mereka agar mengeklik *link*.

KESIMPULAN DAN SARAN

Risiko keamanan pada *Self-Service Technology* Perbankan Syariah merupakan suatu keniscayaan, baik yang dapat diperkirakan maupun yang tidak dapat diperkirakan, dan tentunya berdampak negatif terhadap perbankan syariah. Berdasarkan hasil analisis data yang diperoleh dari observasi lapangan bahwa Bank BJB Syariah telah menerapkan manajemen risiko keamanan *Self-Service Technology* perbankan syariah dengan baik dilihat dari tidak adanya kasus-kasus *Cyber Crime* pada Bank BJB Syariah. Dalam menjalankan manajemen risiko keamanan *Self-Serrvice Technology* perbankan syariah, Bank BJB Syariah memiliki strategi atau cara untuk meminimalisir risiko-risiko tersebut, yaitu dengan cara memberikan edukasi dan kesadaran kepada nasabah agar berhati-hati dalam menggunakan fasilitas Self-Service Technology, seperti; 1) menjaga data atau akun pribadi dengan cara tidak memberikan kode OTP, kode verifikasi ATM dan kode rahasia lainnya; 2) menjaga keamanan data pribadi dengan waspada saat menggunakan wi-fi publik; 3) berhati-hati dengan *link* atau situs palsu. Selain itu Bank BJB Syariah menggunakan sistem keamanan seperti antivirus, sistem *cryptography*, yang berarti melakukan pengamanan komunikasi ataupun informasi menjadi kode rahasia sehingga menjadi lebih aman. Bank BJB Syariah juga melakukan langkah preventif penguatan sistem keamanan teknologi informasi terhadap potensi gangguan data dengan peningkatan proteksi dan ketahanan sistem dan selalu memantau sistem *Self-Service Technology* secara teratur untuk memastikan bahwa tidak ada kelemahan keamanan yang dapat digunakan oleh pihak-pihak yang tidak berwenang.

DAFTAR PUSTAKA

Administrator. (2022). *Pentingnya Manajemen Risiko (Bagian 1)*. Inspektorat.Kulonprogokab.Go.Id. https://inspektorat.kulonprogokab.go.id/detil/1849/pentingnya-manajemen-risiko-bagian-1#:~:text=Menurut Vaughan (1978)%2C beberapa,the uncertainty (risiko adalah ketidakpastian)

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam

Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Ahdiat, A. (2023). *Transaksi Digital Banking di Indonesia Tumbuh 158% dalam 5 Tahun Terakhir*. Katadata.Co.Id. https://databoks.katadata.co.id/datapublish/2023/07/05/transaksi-digital-banking-di-Indonesia-tumbuh-158-dalam-5-tahun-terakhir

Ainulyaqin, M. H., Rakhmat, A. S., Edy, S., & Maharani, S. (2023). Analisis Dana Pihak Ketiga (DPK), Risiko Dan Fee Based Income (FBI) Terhadap Pembiayaan Bagi Hasil Pada Bank Umum Syariah. *Indonesian Journal of Islamic Economics and Business*, *8*(1), 196-207.

Akuntansi, J., Fajri, A. M., Violita, E. S., Indonesia, U., & Author, C. (2023). *Analisis Manajemen Risiko Bank Syariah Dalam Melakukan Transformasi Digital (Studi Kasus Pada Bank AS)*. *7*(April), 1249–1258.

Andrian, S., Eriani, D., & Faisal, F. (2023). Perlindungan Hukum Bagi Nasabah Pengguna Mobile Banking Pt.Bank Syariah Indonesia Unit Kcp Chik Johan Ditinjau Dari Undang-Undang Nomor 08 Tahun 1999 Tentang Perlindungan Konsumen. *REUSAM: Jurnal Ilmu Hukum*, *11*(1), 1. https://doi.org/10.29103/reusam.v11i1.11158

Arnita, N., Yarmunida, M., & Sumarni, Y. (2023). Pengaruh Self Service Technology (Sst) Terhadap Kepuasan Nasabah Pengguna Layanan Digital (Study Kasus Bank Syariah Indonesia). *Jurnal Tabarru': Islamic Banking and Finance*, *6*(1), 72–80. https://doi.org/10.25299/jtb.2023.vol6(1).12784

Azizah, A. N., Santoso, K. A., & Jember, U. (n.d.). *PENENTUAN LOKASI ATM BANK SYARIAH INDONESIA*.

Cantika, Y. (2021). *Pengertian Bank Syariah beserta Fungsi hingga Ciri-nya!* Gramedia.Com. https://www.gramedia.com/literasi/syajaah/

Damara, D. (2021). *Bank Umum RI Boncos Rp246,5 Miliar karena Serangan Siber, Kok Bisa?* Bisnis.Com. https://finansial.bisnis.com/read/20211026/90/1458617/bank-umum-ri-boncos-rp2465-miliar-karena-serangan-siber-kok-bisa

Dihni, V. A. (2022). *Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022*. Katadata.Co.Id. https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocoran-data-di-Indonesia-melonjak-143-pada-kuartal-ii-2022

hidayat fahrul, D. (2023). *Pengaruh Marketing Mix Dan Self Service Technology Terhadap Loyalitas Nasabah Bank Muamalat Kantor Cabang Malang*. *2*(2), 31–41. https://doi.org/10.55123/jumintal.v2i2.2231

Keuangan, J. L., & Islam, B. (2023). *Asy-Syarikah Asy-Syarikah*. *5*(2), 87–100.

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam

Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Keuangan, O. J. (2023). *Undang-undang Nomor 21 Tahun 2008 Tentang Perbankan Syariah*. Ojk.Go.Id. https://ojk.go.id/id/kanal/syariah/regulasi/undang-undang/Pages/undang-undang-nomor-21-tahun-2008-tentang-perbankan-syariah-2.aspx#:~:text=Undang-undang Nomor 21 Tahun 2008 Tentang Perbankan Syariah,-16 Juli 2008&text=Ketentuan fungsi bank syariah juga,ke

Leviani, N., & Wiyono, S. (2023). Pengaruh Mobile Banking, Internet Banking, Non Performing Loan Dan Biaya Operasional Pendapatan Operasional Terhadap Profitabilitas Return on Asset Bank Pada Perusahaan Perbankan Yang Terdaftar Di Bei Tahun 2017 – 2021. *Jurnal Ekonomi Trisakti*, *3*(1), 1613–1622. https://doi.org/10.25105/jet.v3i1.16213

Marcelliana, V., & dkk. (2023). Penerapan Perlindungan Konsumen Terhadap Nasabah PT. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah. *Deposisi: Jurnal Publikasi Ilmu Hukum*, *1*(2), 180–194. https://journal.widyakarya.ac.id/index.php/Deposisi-widyakarya/article/view/577

Nasruron, M., & Safitri, N. A. A. (2021). Analisis Perkembangan Perbankan Syariah Di Indonesia Di Masa Pandemi Covid-19. *Al Birru: Jurnal Keuangan Dan …*, *I*(1), 1–20. http://jurnal.iaihnwpancor.ac.id/index.php/albirru/article/view/525

Natalia, T. (2023). *Deretan Kasus Siber di Sektor Keuangan, Ada BFIN hingga BPJS*. CNBC Indonesia. https://www.cnbcIndonesia.com/market/20230525100046-17-440427/deretan-kasus-siber-di-sektor-keuangan-ada-bfin-hingga-bpjs

Nelly, R., Siregar, S., & Sugianto, S. (2022). Analisis Manajemen Risiko Pada Bank Syariah: Tinjauan Literatur . *Reslaj : Religion Education Social Laa Roiba Journal*, *4*(4), 918–930. https://doi.org/10.47467/reslaj.v4i4.1008

Novi. (2021). *Manajemen Risiko: Pengertian, Manfaat, Tujuan, Prinsip dan Langkah-langkahnya*. Gramedia.Com. https://www.gramedia.com/literasi/manajemen-risiko/

Pratama, G. (2023). *Perbankan RI Sasaran Empuk Serangan Siber, Ini Faktanya*. Infobanknews.Com. https://infobanknews.com/perbankan-ri-sasaran-empuk-serangan-siber-ini-faktanya/

Rakhmat, A. S., Fahamsyah, M. H., Nurastuti, P., & Ainulyaqin, M. H. (2023). Integrating Banking Fundamental Factors with Financial Technology in Reducing Banking Risk. *East Asian Journal of Multidisciplinary Research*, *2*(9), 3567-3572.

Rakhmat, A. S., Fahamsyah, M. H., Nurastuti, P., & Ainulyaqin, M. H. (2024). Integrating Banking Fundamental Factors with Financial Technologies in Increasing Banking Performance. *Ilomata International Journal of Management*, *5*(1), 251-260.

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam

Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Ramadhanti, M., Shodiq, N., & Mawardi, M. C. (2022). Pengaruh Digitalisasi Perbankan Melalui Self-Service Technology Terhadap Kepuasan Mahasiswa Unisma Dalam Penggunaan Layanan Digital Bank Syariah (Studi Kasus Pada Mahasiswa FEB UNISMA Angkatan 2018 dan 2019). *Junral El-Aswaq*, *3*, 1–15. http://riset.unisma.ac.id/index.php/laswq/article/view/17988

Rangkuti, M. (2023). *Manajemen Risiko Pengertian, Ciri, Tujuan, Manfaat, dan Prinsip*. Feb.Umsu.Ac.Id. https://feb.umsu.ac.id/manajemen-risiko-pengertian-ciri-tujuan-manfaat-dan-prinsip/

Rini, A. S. (2023). *Daftar Kasus Kebocoran Data Sektor Finansial RI Selain BSI (BRIS)*. Bisnis.Com. https://finansial.bisnis.com/read/20230516/90/1656438/daftar-kasus-kebocoran-data-sektor-finansial-ri-selain-bsi-bris

Rochmah, S., & Ernawati, F. Y. (2022). Pengaruh Layanan Automatic Teller Machine (ATM), Internet Banking, Dan Mobile Banking Terhadap Tingkat Kepuasan Nasabah. *Jurnal Ilmiah Infokam*, *18*(1), 18–27. https://doi.org/10.53845/infokam.v18i1.315

Sihabudin, F., Achmad, L. I., Hamdan'Ainulyaqin, M., Midisen, K., & Edy, S. (2022). Analysis of Blockchain Technology and Security Principles in Cryptocurrency Transactions according to the perspective of Islamic Economics: Case study: Smart Contract on the Ethereum Blockchain Network. *Ta'amul: Journal of Islamic Economics*, *1*(1), 11-20.

Solihin, K., & Kurniawan, F. A. (2022). *Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security*. *1*, 1–20.

Suhaemin, A., & Muslih, M. (2023). Karakteristik Cybercrime di Indonesia. *Edulaw: Journal of Islamic Law and Jurisprudance*, *5*(2), 15–26.

Tartila, M. (2022). Strategi Industri Perbankan Syariah dalam Menghadapi Era Digital. *Jurnal Ilmiah Ekonomi Islam*, *8*(03), 3310–3316.

Times, S. intern I. (2023). *Risiko: Pengertian Menurut Ahli serta Jenis-jenisnya*. Idntimes.Com. https://www.idntimes.com/business/economy/seo-intern-idn-times/risiko-pengertian-menurut-ahli-serta-jenis-jenisnya

Ula, R. No. Z., Maslichah, & Junaidi. (2022). Technology Terhadap Kepuasan Mahasiswa Pengguna Layanan Digital Bank Syariah. *El-Aswaq: Islamic Economic and Finance Journal*, *3*(2), 178–191.

Wareza, M. (2021). *Awas! 3 Masalah Ini Rentan Hantui Bank-bank Digital RI*. CNBC Indonesia. https://www.cnbcIndonesia.com/market/20211026145711-17-286662/awas-3-masalah-ini-rentan-hantui-bank-bank-digital-ri

El-Mãl | Jurnal Kajian Ekonomi & Bisnis Islam
Vol 5 No 7 (2024) 3564 – 3578 P-ISSN 2620-295 E-ISSN 2747-0490
DOI: 1047467/elmal.v5i7.3379

Yolandha, F. (2021). *menengok fenomena bank digital*. Republika. https://ekonomi.republika.co.id/berita/qz3uhv370/menengok-fenomena-bank-digital