

# **Dampak serangan siber dan kebocoran data pada perbankan syariah terhadap tingkat kepercayaan nasabah**

**Ivan Rizal Nur Ardhian**

Program Studi Akuntansi, Universitas Islam Negeri Maulana Malik Ibrahim Malang

e-mail: 220502110108@student.uin-malang.ac.id

---

## **ABSTRAK**

**Kata Kunci:**

Serangan dunia maya; kepercayaan; nasabah; perbankan syariah

**Keywords:**

Cyber attack; trust; customers; islamic bank

Bank merupakan lembaga keuangan yang berperan penting bagi perekonomian Indonesia saat ini, penggunaan perbankan semakin berkembang karena segala sesuatu yang berkaitan dengan transaksi bank dapat dilakukan dengan menggunakan telepon seluler, Web Banking, mesin ATM, dan teller di kantor-kantor bank. Dari mulai dengan kebutuhan sehari-hari dan melibatkan mereka untuk pertukaran dengan nasabah individu dari bank sejenis atau lainnya. Secara moral, lembaga keuangan ini harus melindungi informasi keamanan klien yang menggunakan layanan mereka. Namun tidak dapat dipungkiri bahwa masih ada kejadian kebocoran informasi, salah satunya yang dialami oleh Bank Syariah X dan jelas mengabaikan standar keamanan informasi, perlindungan informasi dan moral. Adanya dasar pemikiran pembobolan informasi menyebabkan kekurangan klasifikasi, perlindungan, dan aksesibilitas, Bank Syariah X dan menimbulkan kerugian baik materi maupun non materi. Kajian ini bermaksud menerapkan jaminan halal bagi pembeli Bank Syariah X dan kewajiban pelaku usaha terhadap nasabah dalam administrasi keuangan di Bank Syariah X. Dengan mengangkat isu ini, diharapkan secara umum kita akan lebih waspada terhadap bahaya serangan digital yang menggerogoti bisnis keuangan, termasuk perbankan syariah.

---

## **ABSTRACT**

Banks are monetary organizations that assume a significant part for the Indonesian economy as of now, the utilization of banking is expanding on the grounds that everything should be possible utilizing cell phones, Web Banking, ATM machines, and tellers at bank office workplaces. From beginning with day to day needs and involving them for exchanges with individual clients of a similar bank or others. Morally, these financial establishments ought to safeguard the security information of clients who utilize their administrations. Nonetheless, it can't be rejected that there are instances of information spillage, one of which was capable by Bank Syariah X and obviously disregards the standards of information security, information protection and morals. The presence of an information burglary rationale causes a deficiency of classification, protection, accessibility, and respectability of Bank Syariah X and causes misfortunes both material and non-material. This study means to apply lawful security for purchasers of Bank Syariah X and the obligations of business entertainers towards customers in financial administrations at Bank Syariah X. By raising this issue, it is trusted that we will be generally more mindful of the dangers of digital assaults that undermine the financial business, including sharia banking.

---

## **PENDAHULUAN**

Dari segi kualitas produk, layanan yang diberikan, dan iklan berskala besar, pertumbuhan perbankan di Indonesia telah menyita perhatian masyarakat sehingga

mendorong para perusahaan – perusahaan bisnis bersaing untuk mendapatkan kepuasan dan pelayanan terbaik untuk menarik minat nasabah. Menyimpan uang serta kemudahan dalam bertransaksi adalah tujuan utama bank. Kini, perbankan Indonesia juga melakukan hal yang sama. kemajuan komunikasi dan teknologi untuk mendukung pertumbuhan Mobile Banking (Fatah dkk., 2023; Kartika & Segaf, 2022). Mobile Banking sendiri adalah layanan bank yang memungkinkan nasabah untuk melakukan transaksi secara online. Dalam Mobile Banking itu sendiri ada berbagai macam fasilitas yang bisa digunakan oleh nasabah diantaranya yaitu transfer dana, informasi saldo, mutasi rekening, pembayaran listrik rumah, isi pulsa dan masih banyak lagi fasilitas yang ditawarkan oleh Mobile Banking, oleh karenanya Mobile Banking menjadi suatu alat yang dibutuhkan di era modern seperti ini mengingat kegunaannya yang sangat luas (Tambunan dkk., 2023).

Sistem perbankan yang didirikan berdasarkan prinsip syariah, atau hukum Islam, dikenal sebagai perbankan Islam. Riba (bunga) dan praktik lain yang bertentangan dengan hukum syariah dilarang di perbankan Islam. Keuntungan di perbankan Islam diperoleh melalui sistem bagi hasil dan transaksi bisnis yang mengikuti hukum Islam (Marcelliana dkk., 2023).

Selain itu ada risiko yang berkaitan dengan penggunaan *internet banking*, terlepas dari betapa nyamannya layanan ini bagi nasabah. Terdapat berbagai resiko, salah satunya yaitu pelanggaran hukum yang berkaitan dengan masalah pencurian data pribadi dan pencurian uang nasabah. Seiring dengan bahaya yang terkait dengan pencurian data pribadi, nasabah bank juga diresahkan dengan resiko finansial yang menyertai tindak kejahatan ini. Semua itu adalah resiko yang terkait dengan penggunaan perbankan online karena ulah para pelaku kejahatan teknologi informasi. Jenis kejahatan ini sering disebut sebagai "Cyber Crime" dalam konteks teknologi informasi. Tindak kejahatan ini biasanya menggunakan komputer canggih dan teknologi digital untuk tujuan terorisme dan pencucian uang (Arofah dkk., 2020).

Untuk memberikan akses yang lebih cepat dan mudah kepada nasabah, Bank Syariah yang beroperasi sebagai lembaga keuangan sesuai aturan syariah telah memasukkan layanan perbankan digital. Hal yang sama berlaku untuk lembaga keuangan lainnya. Di sisi lain Bank syariah juga rentan terhadap gangguan yang disebabkan serangan hacker dengan menyerang titik vital Bank Syariah yaitu pada layanan online mereka. Pencurian data dari pelanggan adalah salah satu jenis serangan hacker tersebut. Tindak kejahatan hacker lainnya juga meliputi gangguan sistem perbankan atau pencurian uang nasabah. Bersamaan dengan serangan hacker pada Bank Syariah juga membuat tingkat kepercayaan nasabah pada Bank Syariah mulai berkuraang. Selain itu, akibat dari serangan ini, Bank Syariah mengalami kerugian secara financial dan rusaknya reputasi di mata para nasabah (Marcelliana dkk., 2023).

Undang – Undang Perlindungan Konsumen Indonesia (UUPK) bertujuan untuk melindungi konsumen (nasabah), khususnya mereka yang melakukan transaksi perbankan secara online dengan Bank Syariah. UUPK menawarkan kerangka hukum yang komprehensif untuk melindungi hak dan kepentingan konsumen (nasabah) dalam keadaan seperti ini. Nasabah Bank Syariah memiliki hak atas keamanan, dan bank diharuskan untuk menegakkan keamanan sistem perbankan mereka dan

mempertahankan informasi data diri nasabah dari ancaman kejahatan teknologi informasi. Selain itu, konsumen (nasabah) berhak atas informasi yang akurat, maka Bank Syariah dituntut untuk memberikan informasi yang jujur dan terbuka dengan nasabah tentang gangguan layanan digital yang diretas oleh hecker. UUPK juga memberikan pilihan kepada nasabah untuk menerima ganti rugi jika mengalami kerugian akibat pelanggaran bank. Nasabah memiliki hak untuk menerima kompensasi jika mereka percaya bahwa perusahaan telah melanggar hak mereka sebagai konsumen. Nasabah juga berhak mendapatkan ganti rugi yang sebanding dengan kerugian yang telah mereka alami. Bersamaan dengan hak – hak tersebut, UUPK juga menetapkan persyaratan bagi Bank Syariah untuk menjaga dan menjunjung tinggi hak – hak konsumen serta menjaga keamanan sistem perbankan. Langkah – langkah keamanan juga harus memadai dan bisa diterapkan oleh bank – bank Islam, sehingga bisa mengantisipasi serangan siber dan melindungi klien dari potensi bahaya sebagai akibat dari gangguan layanan digital (Marcelliana dkk., 2023).

Namun serangan siber dewasa ini semakin manjadi – jadi yang mengancam data nasabah seperti pada kasus kebocoran data nasabah PT Bank Syariah Indonesia Tbk (BSI) pada 8 Mei 2023. Serangan siber ini masih sering terjadi dan mengancam keamanan data nasabah Bank Syariah. Dampaknya Bank Syariah menghadapi kesulitan dalam layanan digital seperti, mesin ATM, BSI Mobile, dan layanan lainnya di kantor cabang yang sulit untuk diakses. Setelah itu, pada 9 Mei 2023, manajemen BSI memberi pernyataan bahwa masalah tersebut terjadi karena BSI sedang melakukan *maintenance*. BSI juga menyatakan penyesalan atas ketidaknyamanan yang disebabkan oleh *maintenance* ini yang pada akhirnya membuat nasabah tidak bisa melakukan transaksi di Bank Syariah baik online maupun offline. Kenyataanya setelah layanan dianggap pulih, beberapa nasabah masih mengeluhkan adanya gangguan pada layanan Bank Syariah. Sejak adanya laporan tersebut, BSI terus melakukan upaya normalisasi layanannya. Hasilnya, layanan dapat dilanjutkan tetapi secara bertahap. Hery Gunardi selaku Direktur Utama BSI mengatakan bahwa adanya temuan dugaan serangan cyber yang mengganggu layanan BSI. Karena itu, beberapa layanan perusahaan dievaluasi dan dimatikan untuk sementara (Marcelliana dkk., 2023).

Ternyata terungkap bahwa kelompok hacker peretas data – data Bank Syariah adalah LockBit. Kelompok hacker ini meretas data klien BSI dan menyebarkannya di dark web (pasar gelap internet). Selain itu, Lockit juga mengajukan penawaran kepada BSI sebesar Rp 295,61 miliar sebagai uang jaminan agar data para nasabah Bank BSI agar tidak disebarluaskan. BSI mengakui adanya serangan hacker yang berhasil membobol sistem mereka. BSI terus melakukan evaluasi, dan mematikan sistem layanan untuk sementara. LockBit telah berhasil mencuri sekitar 1,5 terabyte data internal BSI, diantara data – data yang telah berhasil dicuri oleh LockBit ada sekitar 15 juta data pribadi nasabah BSI di dalamnya. Data – data pribadi nasabah yang dicuri diantaranya saldo rekening, riwayat saldo, nama, nomer ponsel, riwayat transaksi, tanggal pembukaan rekening, alamat dan beberapa data penting lainnya (Marcelliana dkk., 2023).

Menurut (Arofah dkk., 2020) kejahatan cyber crime ini akan berdampak besar pada Bank Syariah Indonesia yang terkena serangan kejahatan ini. Adapun dampaknya akan mempengaruhi banyak hal yang sifatnya merugikan pihak Bank Syariah Indonesia salah

satunya adalah kepercayaan pelanggan yang berkurang atau lebih sering dikenal dengan adanya risiko reputasi. Di sisi lain Bank Syariah Indonesia juga melakukan upaya lebih untuk perbaikan asset dan perbaikan fisik yang tentunya juga membutuhkan dana yang tidak sedikit. Anggoro Budi Nugroho, pengamat ekonom SBM ITB, mengklaim dugaan peretasan data nasabah BSI oleh peretas menjadi preseden negatif bagi perbankan di Indonesia. Keadaan ini menunjukkan bahwa sektor perbankan Indonesia tidak aman dari segi keamanan teknologi (Maulana A, 2023). Banyak nasabah yang mulai meragukan tentang sistem keamanan di Bank Syariah Indonesia akibat dari pencurian data yang dilakukan oleh sekelompok hacker yang menamai kelompok mereka sebagai LockBit. Bank Syariah Indonesia terus melakukan berbagai upaya pemulihan serta meningkatkan sistem keamanannya, selain daripada itu Bank Syariah Indonesia juga memberikan kompensasi kepada nasabah yang terkena dampak dari tindak kejahatan teknologi ini.

## PEMBAHASAN

Bank syariah didefinisikan sebagai lembaga keuangan yang menjalankan operasinya sesuai dengan hukum syariah. Mereka dapat diklasifikasikan sebagai bank umum syariah atau bank keuangan rakyat syariah berdasarkan jenisnya. Menurut Siamat, Dahlan (2004), bank syariah adalah bank yang menjalankan bisnis sesuai dengan hukum atau prinsip syariah dengan tetap berpegang pada Al-Quran dan Al-Hadits. (Sebtianita E, 2015) Ada berbagai jenis layanan transaksi yang tersedia di industri perbankan syariah antara lain setor tunai, tarik tunai, transfer uang, kliring, dan lain – lain. Nasabah terus melakukan semua transaksi di kantor bank syariah hingga saat ini. Oleh sebab ketika konsumen melakukan beberapa aktivitas perbankan secara offline (di tempat), nasabah lain juga menunggu lebih lama untuk giliran mereka pada waktu yang sama untuk dilayani oleh petugas bank. Seorang petugas bank membutuhkan waktu yang sangat lama untuk melayani nasabah, apalagi ditambah dengan banyaknya nasabah yang sedang mengantri. Ini menimbulkan masalah bagi nasabah dikarenakan waktu mereka yang terbuang sia – sia karena lamanya pelayanan di bank. Selain itu masalah ini juga berdampak buruk bagi bank, bank mau tidak mau harus menambah lebih banyak layanan Counter Teller, ruangan yang diperluas serta penambahan tempat duduk yang tentunya hal ini menjadi penambahan biaya operasional bagi pihak bank.

Teknologi informasi saat ini berkembang dengan sangat pesat, khususnya di industri perbankan konvensional maupun syariah. Dengan kemajuan teknologi informasi, perbankan telah menciptakan layanan yang memudahkan transaksi. Misalnya, industri perbankan baru – baru ini mengembangkan sistem layanan seluler yang disebut *M-Banking*, salah satu produk atau layanan yang memungkinkan nasabah bank melakukan transaksi keuangan melalui gadget tanpa harus datang ke bank secara langsung. Seiring dengan memastikan keamanan dan kerahasiaan yang penting, tujuan lain dari *Mobile Banking* adalah memberikan kenyamanan dan kemudahan untuk nasabah bertransaksi tanpa harus datang langsung dan menunggu di bank. Ini menjadi suatu faktor penting dibuatnya suatu sistem *Mobile Banking* (Priyadi, 2023).

Terlepas dari manfaat *Mobile Banking* yang begitu berdampak besar bagi banyak orang, ternyata sistem yang dikembangkan oleh banyak perbankan ini masih banyak

kekurangan didalamnya termasuk keamanan sistemnya yang sering dihack oleh para hacker yang tidak bertanggung jawab. Akibatnya tidak sedikit data – data bank yang dicuri oleh kelompok hacker, termasuk didalamnya data – data pribadi nasabah yang berisi seperti informasi saldo, mutasi rekening, riwayat penarikan dan masih banyak data penting nasabah lainnya yang berhasil dicuri. Masalah ini berdampak pada tingkat kepercayaan nasabah kepada pihak bank yang dinilai telah lalai dalam menjaga data – data pribadi mereka. Ini menjadi suatu tumpuan dan pembelajaran keras kepada pihak bank agar segera bisa segera memperbaiki sistem mereka, agar nantinya para nasabah tidak berpindah ke bank lain yang dinilai memiliki sistem keamanan yang lebih memadai.

Gambar 1.1 10 Provinsi Dengan Serangan Siber Terbanyak Di Indonesia



Gambar 1.10 Provinsi Dengan Kasus Serangan Siber Terbanyak

Sumber : goodstats.id

Dapat dilihat dari grafik diatas bahwa di Indonesia sendiri masih marak terjadinya serangan siber. Hal ini dikarenakan masih lemahnya sistem keamanan teknologi informasi di Indonesia. Dengan total 54,313 juta serangan, Riau menjadi provinsi yang paling banyak mengalami serangan siber. Terlepas dari kenyataan bahwa provinsi di Pulau Sumatera mengalami insiden paling banyak, 5 dari 6 provinsi di Pulau Jawa menduduki peringkat teratas dalam daftar 10 provinsi dengan insiden serangan siber terbanyak. Hal ini ditunjukkan dengan berada di posisi kedua, Jakarta mengalami 22,67 juta serangan, disusul Jawa Tengah 14,49 juta serangan, dan Jawa Timur 9,2 juta serangan. Provinsi Jawa Barat dengan total 8,02 juta serangan berada di urutan kelima, diikuti oleh Kalimantan Barat dengan 6,53 juta serangan dan Bali dengan 8,04 juta serangan (Syaharani M, 2023).

Perbankan Indonesia harus mengambil pelajaran dari gangguan layanan baru – baru ini yang mungkin disebabkan oleh serangan cyber – ransomware. Perbankan di Indonesia harus memperkuat pertahanan digitalnya, dikarenakan serangan siber semakin agresif dan kompleks, menurut pakar keamanan siber. Istilah ransomware sendiri lebih sering dikenal sebagai dunia maya. Jika sebuah perbankan yang terkena serangan siber tidak memiliki teknisi IT dan sistem keamanan yang andal, maka akan memerlukan waktu yang lama untuk segera pulih. Serangan siber ini biasa diatasi dengan meningkatkan sistem keamanan data bank dan membuat suatu pertahanan

kode bank yang sukar untuk ditembus agar nantinya data bank tidak mudah untuk dicuri, akan tetapi kelompok siber yang cerdas biasanya melakukan serangan itu secara diam – diam tanpa diketahui oleh sistem keamanan bank dan bisa terdeteksi sistem bank setelah pencurian berhasil dilakukan. Untuk mengembalikan data bank yang telah dicuri, biasanya siber akan meminta uang tebusan sebagai bentuk jaminan atas data yang dicuri supaya tidak disebarluaskan (Tambunan dkk., 2023).

Baru – baru ini salah satu perbankan di Indonesia mengalami serangan siber, perbankan itu adalah Bank Syariah Indonesia. Bank Syariah Indonesia (BSI) terkena serangan siber pada tanggal 8 Mei 2023. Dugaan serangan siber dengan menggunakan ransomware yang dilakukan oleh sekelompok hacker bernama LockBit Ransomware Group menyebabkan terganggunya layanan Bank Syariah Indonesia (BSI) beberapa waktu lalu. Peristiwa tersebut menjadi pembelajaran yang sangat berharga bagi industri perbankan Indonesia untuk mulai lebih memperhatikan keamanan sistem yang digunakan, menurut anggota Komisi XI DPR RI Mukhamad Misbakun (KOMISI XI, 2023).

Layanan Bank Syariah Indonesia (BSI) sempat mengalami kelumpuhan selama beberapa hari akibat dari serangan siber, akibatnya banyak nasabah yang mengeluhkan akan masalah gangguan layanan ini. BSI mengatakan layanan akan berangsur membaik dan segera pulih. Hery Gunardi selaku direktur Bank Syariah Indonesia (BSI) mengatakan bahwa layanan BSI akan segera mungkin untuk pulih, beliau juga menambahkan bahwa prioritas Bank Syariah Indonesia adalah menjaga data pribadi dan dana milik nasabah (Hidayatullah, 2023). Pada awalnya, BSI mengklaim bahwa masalah tersebut terjadi karena pemeliharaan sistem sedang dilakukan pada saat itu, sehingga layanan tidak dapat diakses untuk sementara. Pada 14 Mei 2023, ditemukan bahwa serangan ransomware oleh sekelompok peretas sebenarnya yang menyebabkan gangguan layanan BSI. Suatu bentuk perangkat lunak berbahaya yang dikenal sebagai ransomware mengenkripsi data dan mengunci akses ke sistem komputer korban untuk meminta uang tebusan. Para pelaku ransomware, Lock Bit memberikan waktu 72 jam kepada manajemen bank untuk menghubungi mereka. Mereka sangat serius, jika tuntutan mereka tidak dipenuhi, para peretas ini mengancam akan merusak reputasi bank secara keseluruhan. Seolah – olah meremehkan ancaman para peretas ini, manajemen BSI malah mengatakan bahwa layanannya sedang dalam proses pemeliharaan. Dan pada akhirnya sistem perbankan BUMN ini dijangkiti virus yang telah disebarluaskan oleh hacker yang kemudian menyandera data konsumen (Azarine, 2023).

Menurut (Rahayu P, 2020), salah satu cara kerja bank syariah untuk bersaing dengan sesama bank syariah lain dan bank umum (konvensional) adalah dengan memberikan pelayanan yang lebih baik. Untuk memberikan kemudahan dalam pelayanan kepada masyarakat dan pada akhirnya mengajak lebih banyak masyarakat untuk memanfaatkan layanan bank syariah, maka pelayanan baik yang diberikan bank syariah perlu ditingkatkan melalui inovasi layanan. Melalui mekanisme layanan yang terintegrasi dengan internet atau lebih sering dikenal dengan internet banking (electronic banking), salah satu cara untuk meningkatkan pelayanan prima. Di era digital saat ini, layanan internet banking (i-Banking) merupakan salah satu jenis layanan yang efektif untuk membantu bank dalam memberikan layanan kepada nasabahnya. Akan tetapi akibat imbas dari kejahatan teknologi yang dilakukan oleh kelompok siber LockBit

ini membuat tingkat kepercayaan nasabah kepada Bank Syariah Indonesia (BSI) mengalami penurunan yang sangat tajam. Hal ini tentunya membuat membuat manajemen BSI harus memutar otak supaya nasabah tidak lari ke bank lain yang dinilai lebih kredibel (dapat dipercaya). Sistem harus benar-benar bebas dari malware atau trojan apa pun yang dapat digunakan peretas untuk mendapatkan akses, menurut pihak BSI. Cadangan data juga harus diperhitungkan karena ini akan menjadi alat utama untuk memulihkan sistem jika terjadi gangguan. Pratama mendesak Presiden Joko Widodo segera membentuk lembaga perlindungan data pribadi sesuai amanat undang – undang perlindungan data pribadi guna melindungi masyarakat jika terjadi kebocoran data pribadi lagi. Sehubungan dengan kerugian yang menjadi tanggung jawab perusahaan dalam hal ini, Bank Syariah Indonesia wajib mengganti kerugian yang diderita nasabahnya akibat serangan siber ini. Upaya ini dilakukan sebagai bentuk usaha agar nantinya nasabah bisa memberikan rasa kepercayaan mereka lagi terhadap BSI. Oleh karena itu, dengan menggunakan kekayaan Perusahaan ini, Bank Syariah Indonesia sebagai badan hukum harus mempertanggungjawabkan kerugian nasabahnya (Shidiq Mukmin dkk., 2023).

Oleh karena itu, dapat dikatakan bahwa kepercayaan memiliki dampak yang sangat besar terhadap kepuasan nasabah terhadap pengalaman menggunakan mobile banking mereka dengan layanan BSI. Tanpa kepercayaan nasabah, akan membuat nasabah tidak mau melakukan transaksi secara online lagi di BSI, sehingga BSI harus membangun kepercayaan nasabah dengan meningkatkan keamanan layanan digitalnya serta memberikan jaminan dan keamanan kepada nasabah saat melakukan transaksi melalui layanan mobile banking. Hal ini juga yang menjadi faktor penting yang perlu diperhatikan karena sulitnya nasabah dalam memilih dan mempercayakan keuangan tabungannya kepada bank lain (Masruroh A, 2022).

Karena hal ini dapat mempengaruhi kepercayaan nasabah, perlindungan nasabah yang menggunakan e-banking merupakan faktor yang sangat penting. Nasabah yang telah percaya pada layanan e-banking melakukannya tanpa merasa terintimidasi. Perlindungan pelanggan di sisi lain, adalah mengambil langkah-langkah untuk memastikan nasabah merasa aman saat bertransaksi. Nasabah harus dapat mengandalkan bank untuk menjunjung tinggi keamanan bank, agar bank tetap mendapatkan kepercayaannya (Madaniah Nasution & Suprayitno, 2022).

## Kesimpulan dan Saran

Perkembangan teknologi dan informasi dewasa ini sangat cepat. Berbagai sektor kehidupan mulai melek terhadap perkembangan teknologi saat ini, mulai dari sektor ekonomi, sektor pertanian, sektor industri pabrik, sektor perkantoran dan masih banyak lainnya. Kemajuan teknologi sangat berpengaruh terhadap lini kehidupan saat ini, termasuk dalam sektor perekonomian khususnya pada bank. Inovasi kemajuan teknologi dalam perbankan salah satunya yaitu adanya inovasi *mobile banking* (*m-banking*), inovasi ini memungkinkan para nasabahnya untuk bertransaksi tanpa harus datang langsung ke bank (online). Adanya inovasi ini dilatarbelakangi oleh nasabah yang mengeluhkan tentang lamanya layanan pada perbankan yang dinilai membuang – buang waktu, serta tidak efisien, akhirnya dibuatlah inovasi teknologi ini. Akan tetapi dibalik itu

semua tentu juga ada kelemahan, kelemahan dari mobile banking ini adalah sistemnya yang gampang sekali untuk dihack oleh pelaku kejahatan siber. Seperti pada kasus Bank Syariah Indonesia baru – baru ini yang sistemnya terkena hack oleh kelompok siber bernama LockBit, akibatnya data – data BSI sebesar 1,5 terabyte berhasil dicuri. Hal ini tentunya berdampak pada nasabah, dimana nasabah mulai meragukan sistem keamanan di BSI dan tingkat kepercayaan nasabah pada BSI semakin menurun. Akhirnya untuk mengembalikan kepercayaan nasabah pada BSI, BSI melakukan upaya penggantian rugi kepada para nasabah dan akan terus meningkatkan sistem keamanan dan layanan BSI.

Masalah ini sangat berdampak pada aktivitas keuangan di daerah yang khususnya sangat begantung pada Bank X. Oleh sebab itu penulis memberikan saran kepada Bank X yaitu :

- 1) Bank X khususnya pada manajemennya jangan terlalu menganggap remeh persoalan kecil, karena persoalan yang dianggap kecil nyatanya bisa menjadi masalah besar.
- 2) Bank X harus terus meningkatkan layanan dan inovasi terbaru supaya nasabah semakin merasa nyaman untuk bertransaksi di BSI.
- 3) Bank X juga harus melakukan evaluasi terkait sistem keamanannya agar tidak mudah dihack oleh pelaku kejahatan teknologi.

## Daftar Pustaka

- Arofah, N. R., Priatnasari, Y., Nida, O. ;, & Arofah, R. (2020). Internet banking dan cyber crime : sebuah studi kasus di perbankan nasional internet banking and cyber crime: a case study in national banking. Dalam *Jurnal Pendidikan Akuntansi Indonesia* (Vol. 18, Nomor 2).
- Azarine, A. (2023, Mei 18). *Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah*. lk2fhui.law.ui.ac.id.  
<https://lk2fhui.law.ui.ac.id/portfolio/bank-bsi-pasca-serangan-siber-mengungkap-potensi-kompensasi-bagi-nasabah/>
- Fatah, M. I., Asnawi, N., Segaf, S., & Parmujianto, P. (2023). Case study at KSPPS BMT UGT nusantara Indonesia an analysis of using mobile applications to increase fee-based income. *Enrichment: Journal of Management*, 13(2), 1182–1191.
- Hidayatullah. (2023, Mei 16). *BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank “tidak kuat.”* bbc.com.  
<https://www.bbc.com/indonesia/articles/cno1gdr7eero>
- Kartika, G., & Segaf, S. (2022). Kombinasi Peran Model TAM dan CARTER Terhadap Optimalisasi Kepuasan Nasabah Mobile Syariah Banking di Masa Pandemi Covid-19. *Jurnal Manajerial*, 9(02), 152–167.
- KOMISI XI. (2023, Mei 16). *Kasus Serangan Siber BSI Jadi Pelajaran Mahal bagi Sistem IT Perbankan*. dpr.go.id.  
<https://www.dpr.go.id/berita/detail/id/44513/t/Kasus+Serangan+Siber+BSI+Jadi+Pelajaran+Mahal+bagi+Sistem+IT+Perbankan>
- Madaniah Nasution, A., & Suprayitno, E. (2022). Pengaruh Penggunaan E-Banking dan Perlindungan Nasabah Terhadap Kepercayaan Nasabah dengan Literasi

- Keuangan sebagai Variabel Moderasi. *Jurnal Ilmiah Ekonomi Islam*, 8(02), 1205–1213. <https://doi.org/10.29040/jiei.v8i2.4595>
- Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., Sukarto, M., Fitriani, C. N., Alief, T., & Bayhaqi, R. (2023). Penerapan perlindungan konsumen terhadap nasabah PT. Bank Syariah Indonesia dalam kasus kebocoran data nasabah. 1(2), 180–194. <https://doi.org/10.59581/depositi.v1i2.562>
- Masruroh A. (2022). Pengaruh Eservice quality dan Trust Terhadap Keputusan Penggunaan Layanan Syariah Link Aja serta Dampaknya pada Kepuasan Konsumen. <https://repository.uinjkt.ac.id/dspace/handle/123456789/72864>
- Maulana A. (2023, Mei 6). Data BSI Diduga Diretas Hacker, Kepercayaan Nasabah Bisa Merosot! ayobandung.com. <https://www.ayobandung.com/bisnis/798773897/data-bsi-diduga-diretas-hacker-kepercayaan-nasabah-bisa-merosot>
- Priyadi, W. (2023). Cara sitasi: Wiwit Priyadi. 2023. Analisis Cyber Security Pada Pengguna Mobile Banking Di Indonesia. *Bina Insani ICT Journal*, 10(1), 278–289. [https://tekno.kompas.com/\[6\].](https://tekno.kompas.com/[6].)
- Rahayu P. (2020). Pengaruh persepsi kemudahan dan risiko terhadap minat transaksi dengan menggunakan i-banking (studi pada mahasiswa Universitas Islam Negeri Maulana Malik Ibrahim Malang). <http://etheses.uin-malang.ac.id/id/eprint/18288>
- Sebtianita E. (2015). ANALISIS KINERJA UMUM BANK SYARIAH DENGAN MENGGUNAKAN PENDEKATAN ISLAMICITY PERFORMANCE INDEX (Studi Pada Bank Umum Syariah Periode Tahun 2009 - 2013). *Jurnal Fakultas Ekonomi UIN Malang*. <http://etheses.uin-malang.ac.id/1107/11/11510022%20Ringkasan.pdf>
- Shidiq Mukmin, M., Mukmin, M. S., Jalan, A. ;, Telang, R., Kamal, K., Bangkalan, K., & Timur, J. (2023). Tanggung Jawab Bank Syariah Indonesia Pasca Peristiwa Hacking Yang Merugikan Beberapa Nasabah. 1(3), 83–89. <https://doi.org/10.59246/aladalah.v1i3.335>
- Syaharani M. (2023, Juni 22). Serangan Siber Marak Terjadi Di Indonesia, Provinsi Mana Yang Paling Banyak Terserang? goodstats.id. <https://goodstats.id/article/serangan-siber-marak-terjadi-di-indonesia-provinsi-mana-yang-paling-banyak-terserang-2Kxb2>
- Tambunan, N., Fitri Wulandari, A., Pangesti, A. N., Anggraini, A., Tunjaja, S., Dewi Gita, A., & Rusmarhadi, I. (2023). Berita utama tentang error service di Bank Syariah Indonesia (BSI). *Community Development Journal*, 4(2), 5096–5098.