Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 3, Issue Agustus, 2025 pp. 30-34 http://urj.uin-malang.ac.id/index.php/mij/index

Risiko reputasi akibat kejahatan digital: studi kasus kebocoran data nasabah dan respons publik di media sosial

Indriana Irawati
program studi Perbankan Syariah, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: 220503110050@student.uin-malang.ac.id

Kata Kunci:
kejahatan siber; reputasi digital; media social; kebocoran data; BSI

Keywords:
Cybercrime; digital reputation; social media; data breach; BSI

A B S T R A K

Transformasi digital dalam sektor perbankan telah membawa kemudahan akses layanan keuangan bagi masyarakat, namun di saat yang sama juga meningkatkan risiko kejahatan siber, termasuk kebocoran data pribadi. Studi ini membahas dampak reputasi yang ditimbulkan dari insiden kebocoran data nasabah Bank Syariah Indonesia (BSI) pada tahun 2023, serta bagaimana media sosial memainkan peran penting dalam membentuk persepsi publik. Metode kajian dilakukan melalui studi literatur dan analisis respons publik di platform digital. Hasil pembahasan menunjukkan bahwa respons negatif di media sosial dapat memperburuk citra perusahaan secara cepat dan berdampak jangka panjang terhadap kepercayaan masyarakat. Oleh karena itu, perusahaan perbankan perlu mengembangkan sistem keamanan siber yang tangguh, strategi komunikasi krisis yang efektif, serta pengelolaan reputasi digital secara proaktif melalui media sosial.

A B S T R A C T

The digital transformation in the banking sector has significantly improved public access to financial services, yet it has also increased the risk of cybercrime, including personal data breaches. This study examines the reputational impact caused by the 2023 customer data breach at Bank Syariah Indonesia (BSI), and how social media plays a key role in shaping public perception. The research employs a literature review and public response analysis through digital platforms. Findings indicate that negative reactions on social media can rapidly damage a company's image and have long-term consequences on public trust. Therefore, banking institutions must develop robust cybersecurity systems, implement effective crisis communication strategies, and manage their digital reputation proactively through social media.

Pendahuluan

Kemajuan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk sektor perbankan. Perbankan digital kini menjadi fondasi utama dalam penyediaan layanan keuangan yang lebih cepat, efisien, dan mudah diakses oleh masyarakat. Namun, di balik segala kemudahan yang ditawarkan, perkembangan ini juga memunculkan risiko baru yang tidak kalah serius yakni kejahatan siber.Kejahatan siber atau *cybercrime* mencakup berbagai bentuk tindakan ilegal yang dilakukan melalui jaringan komputer dan internet. Bentuk kejahatan ini sangat beragam, mulai dari peretasan sistem, pencurian data pribadi, pengambilalihan akun, penyebaran *malware*, hingga serangan *ransomware*. Dalam konteks perbankan, kejahatan siber menjadi ancaman serius karena menargetkan

informasi krusial seperti data pribadi, rekening nasabah, serta transaksi keuangan (Restika & Sonita, 2023). Selain kerugian finansial, serangan siber juga dapat merusak integritas data dan menurunkan tingkat kepercayaan masyarakat terhadap institusi keuangan.Data pribadi kini menjadi komoditas yang sangat bernilai tinggi di dunia digital. Setiap nama, alamat, nomor identitas, riwayat transaksi, dan informasi finansial yang dikumpulkan oleh lembaga perbankan merupakan target empuk bagi pelaku kejahatan siber. Ketika data pribadi ini bocor atau disalahgunakan, tidak hanya nasabah yang dirugikan namun juga institusi keuangan tersebut. Dampaknya bisa sangat luas—mulai dari pencurian identitas, penipuan keuangan, hingga kerugian reputasi yang sulit dipulihkan. Oleh karena itu, perlindungan data pribadi menjadi prioritas utama yang tidak bisa ditawar dalam transformasi digital perbankan.

Di sisi lain, media sosial memainkan peran sentral dalam menyebarkan informasi dan menjadi wadah utama bagi masyarakat untuk mengekspresikan pendapat mereka. Ketika terjadi suatu insiden seperti kebocoran data, masyarakat cenderung menyuarakan kekecewaan, keluhan, dan kritik mereka melalui platform-platform digital ini. Dengan sifatnya yang viral dan dapat diakses publik, media sosial memperkuat dampak reputasi dari setiap insiden yang terjadi. Perusahaan tidak hanya dituntut untuk menangani masalah teknis, tetapi juga harus mampu mengelola persepsi publik secara cepat dan tepat.Dengan latar belakang ini, artikel ini akan membahas risiko reputasi yang ditimbulkan akibat kejahatan digital, dengan fokus pada studi kasus kebocoran data nasabah di Bank Syariah Indonesia (BSI) dan bagaimana respons publik melalui media sosial menjadi penentu dalam membentuk citra dan kepercayaan masyarakat terhadap lembaga perbankan.

Risiko Keamanan Siber dalam Era Digital

Serangan siber dapat berbentuk berbagai tindakan yang disengaja maupun tidak disengaja, dilakukan oleh individu atau kelompok, dengan motivasi yang beragam, dan melibatkan sistem elektronik serta jaringan informasi. Kejahatan ini mencakup pencurian identitas, peretasan sistem, manipulasi informasi, dan penyebaran malware (Alfi et al., 2023). Dalam konteks media digital, karakteristik platform yang terdesentralisasi dan keterlibatan tinggi dari pengguna menciptakan tantangan tambahan dalam pengelolaan keamanan.Popularitas media digital juga meningkatkan potensi risiko seperti pencurian akun, penyebaran berita palsu (hoaks), dan penyalahgunaan data pribadi. Data pribadi menjadi aset berharga di era digital dan apabila disalahgunakan, dapat menimbulkan dampak serius seperti penipuan keuangan, pencemaran nama baik, bahkan ancaman terhadap keamanan individu (Putri et al., 2025). Oleh sebab itu, perlindungan data pribadi harus menjadi prioritas dalam strategi pengembangan layanan digital.

Risiko reputasi muncul ketika kepercayaan stakeholder terhadap suatu lembaga menurun akibat pemberitaan negatif atau pengalaman buruk pengguna layanan. Reputasi merupakan aset tak berwujud yang sangat penting dalam dunia perbankan. Namun, membangun reputasi membutuhkan waktu lama, sementara merusaknya bisa terjadi dalam hitungan menit (Fauziah, 2019). Dalam era digital, penyebaran informasi yang sangat cepat, khususnya melalui media sosial, memperparah risiko reputasi saat terjadi insiden seperti kebocoran data.Transformasi digital dalam sektor keuangan telah

mengubah cara masyarakat mengakses layanan perbankan. Digital banking menjadi solusi utama dalam menjawab kebutuhan efisiensi dan kemudahan transaksi. Di Indonesia, Bank Syariah Indonesia (BSI) merupakan salah satu lembaga yang aktif mengembangkan layanan digital untuk nasabah. Namun, digitalisasi juga meningkatkan potensi serangan siber. Data dari IMF menunjukkan bahwa kerugian tahunan sektor keuangan global akibat serangan siber mencapai lebih dari USD 100 miliar atau sekitar Rp 1.433 triliun (Rizky, 2022).Meskipun demikian, laporan National Cyber Security Index (NCSI) menunjukkan bahwa Indonesia berada di posisi lima besar negara dengan keamanan siber terbaik di kawasan ASEAN pada tahun 2023. Namun, masih terdapat sejumlah insiden yang menunjukkan perlunya peningkatan sistem keamanan secara menyeluruh.

Studi Kasus: Serangan Siber terhadap BSI

Pada 8 Mei 2023, layanan digital Bank Syariah Indonesia (BSI) mengalami gangguan besar. Nasabah melaporkan tidak dapat mengakses aplikasi BSI Mobile, ATM, dan layanan di kantor cabang. Awalnya, BSI menyatakan bahwa gangguan disebabkan oleh proses pemeliharaan sistem. Namun, muncul dugaan kuat bahwa telah terjadi serangan siber, dan tidak lama kemudian muncul isu peretasan data oleh kelompok ransomware.BSI mengklaim layanan kembali normal pada 11 Mei 2023, namun banyak nasabah di media sosial menyatakan bahwa gangguan masih berlangsung hingga beberapa hari setelahnya. Pada 16 Mei, BSI menyatakan bahwa data dan dana nasabah tetap aman. Namun, pada 18 Mei, kelompok ransomware LockBit mengaku telah mencuri 1,5 terabyte data dari BSI karena negosiasi pembayaran tebusan yang gagal.

Sebagai respons atas insiden tersebut, BSI mengimplementasikan berbagai langkah strategis untuk memperkuat sistem keamanan digital. Di antaranya adalah penggunaan enkripsi data, otentikasi dua faktor, serta sistem pertahanan berlapis terhadap serangan siber. BSI juga mengalokasikan anggaran sebesar Rp 580 miliar untuk peningkatan sistem digital dan perlindungan data, serta berkoordinasi dengan BSSN, OJK, dan Bank Indonesia (Fatmala Putri et al., 2023).Langkah-langkah ini bertujuan tidak hanya untuk mengatasi insiden yang terjadi, tetapi juga untuk membangun ulang kepercayaan nasabah dan menjaga reputasi lembaga keuangan syariah tersebut. Selain itu, kerja sama dengan instansi pengawasan dan keamanan siber menjadi penting dalam mengembangkan standar ketahanan digital nasional.

Respons Publik di Media Sosial

Media sosial memainkan peran penting dalam membentuk persepsi publik terhadap perusahaan. Ketika terjadi gangguan layanan atau insiden kebocoran data, nasabah cenderung mengungkapkan keluhan, kekecewaan, dan kritik secara terbuka melalui platform digital seperti Twitter, Instagram, atau TikTok. Jejak digital dari komentar ini bersifat permanen dan dapat memperkuat atau merusak citra perusahaan dalam waktu yang sangat singkat. Apa yang dulu hanya menjadi percakapan terbatas kini bisa menjadi isu nasional hanya dalam hitungan jam. Jejak digital dari komentar ini bersifat permanen dan dapat memperkuat atau merusak citra perusahaan dalam waktu singkat.Respons publik yang negatif terhadap layanan BSI pasca-insiden menunjukkan bahwa media sosial bukan hanya saluran informasi, tetapi juga telah menjadi kanal kontrol reputasi

yang kuat. Bahkan satu unggahan viral yang memperlihatkan kekecewaan nasabah dapat memantik gelombang distrust yang luas. Ketika perusahaan gagal merespons dengan cepat dan transparan, publik bukan hanya kecewa—mereka bisa kehilangan kepercayaan sepenuhnya. Tidak cukup hanya merespons, perusahaan juga harus membangun narasi positif dan aktif menciptakan rekam jejak digital yang baik. Ini mencakup publikasi kegiatan sosial, inovasi layanan, dan pelibatan nasabah dalam pengambilan keputusan melalui media sosial. Dalam jangka panjang, reputasi digital yang baik dapat membantu menutup jejak negatif dari masa lalu.

Kondisi ini menunjukkan bahwa membangun kepercayaan publik tidak bisa dilakukan secara instan. Reputasi di media sosial bersifat kumulatif, jika negatifnya lebih sering muncul, maka persepsi publik pun akan terus memburuk. Bahkan, dalam jangka panjang, dampaknya reputasi yang tercoreng bisa memengaruhi minat investor, menurunkan kepercayaan nasabah, hingga menyulitkan perusahaan dalam menjalin kerja sama di masa depan.Karena itu, perusahaan perlu aktif memantau dinamika media sosial dan merespons secara cepat, terbuka, dan empatik. Namun, merespons saja tidak cukup. Perusahaan juga harus mulai membangun citra positif secara konsisten. Ini bisa dilakukan dengan membagikan kegiatan sosial, inovasi layanan, atau membuka ruang diskusi dengan nasabah melalui media sosial. Tujuannya adalah menciptakan jejak digital yang sehat, yang secara perlahan bisa menutup jejak negatif dari masa lalu dan memperkuat kepercayaan di masa depan.

Kesimpulan dan Saran

Insiden kebocoran data yang dialami oleh Bank Syariah Indonesia (BSI) menunjukkan bahwa transformasi digital harus diimbangi dengan peningkatan sistem keamanan siber yang memadai. Risiko reputasi menjadi konsekuensi serius dari kelemahan dalam perlindungan data, terutama ketika respons perusahaan tidak sejalan dengan ekspektasi publik.Dalam konteks ini, perusahaan perlu mengembangkan sistem manajemen risiko yang komprehensif, termasuk strategi komunikasi krisis yang transparan dan responsif. Jejak digital yang terbentuk di media sosial harus dijaga dengan komunikasi yang jujur dan bertanggung jawab. Membangun kepercayaan publik bukan hanya tentang memberikan layanan terbaik, tetapi juga tentang bagaimana perusahaan mengelola krisis dan memperbaiki kesalahan dengan cepat dan tepat.Untuk itu, BSI dan institusi perbankan lain perlu terus mengembangkan infrastruktur keamanan, melakukan audit rutin, melatih SDM untuk tanggap terhadap insiden siber, serta membangun sistem monitoring media sosial sebagai alat kontrol terhadap reputasi digital. Semua ini bertujuan menjaga kepercayaan nasabah, yang merupakan pilar utama keberlangsungan bisnis perbankan di era digital.

Daftar Pustaka

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 5. https://doi.org/10.7454/jkskn.v6i2.10082

Fatmala Putri, D., Andriani, Sari, W. R., & Nabbila, F. L. (2023). Analisis Perlindungan

Nasabah BSI Terhadap Kebocoran Data Dalam Menggunakan Digital Banking. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *1*(4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Fauziah, S. (2019). Manajemen Risiko Reputasi pada Perbankan Syariah Di Indonesia. *EKSISBANK: Ekonomi Syariah Dan Bisnis Perbankan*, *3*(1), 74–80. https://doi.org/10.37726/ee.v3i1.35

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan Online dalam Media Sosial : Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Jurnal Pengabdian Nasional (JPN) Indonesia. *Jurnal Pengabdian Nasional (JPN) Indonesia*, *6*(1), 38–52. https://doi.org/https://doi.org/10.35870/jpni.v6i1.1097

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25. https://doi.org/10.30983/krigan.v1i2.7929

Rizky, M. J. (2022). *No Title*. Hukum Online.com. https://doi.org/https://www.hukumonline.com/berita/a/risiko-dan-langkah-mitigasi-serangan-siber-sektor-perbankan-digital-lt62846d0e25570/