INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 1 Tahun 2024 Page 8244-8258
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Manajemen Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah

Nicky Maulana[1✉], Tito Laurens[2], Didar Hadrian Afzal Faiz[3], Tria Patrianti[4]
Fakultas Ilmu Sosial dan Ilmu Politik, FISIP UMJ, Jakarta Selatan, Indonesia
Email: nickymaulana123@gmail.com[1✉]

Abstrak

PT Bank Syariah Indonesia Tbk merupakan Badan Usaha Milik Negara (BUMN) yang bergerak dibidang perbankan syariah yang sedang mengalami krisis, krisis yang terjadi adalah peretasan data nasabah yang disebabkan oleh sekelompok hacker *Lockbit 3.0*. Tujuan dari penelitian ini adalah untuk mengetahui manajemen krisis yang dilakukan public relations BSI pada kasus peretasan data nasabah dengan menganalisis Manajemen Krisis yang diantaranya, faktor terjadinya krisis tersebut, cara menanggulangi krisis, dan penyelesaian krisis. Penelitian ini menggunakan teori SSCT, Menurut Coombs & Holladay (2010) *Situational Crisis Communication Theory (SCCT)* membagi strategi respon krisis menjadi tiga strategi utama, yaitu : *Deny Strategy, Diminishing Strategy, dan Bolstering Strategy*. penelitian ini menggunakan metode kualitatif deskriptif. Manajemen krisis PT. Bank Syariah Indonesia (BSI) Tbk pasca peretasan data nasabah terbukti responsif dan efektif. BSI mengidentifikasi serangan ransomware Lockbit, meresponsnya dengan transparan melalui press release yang mencakup permintaan maaf, tanggung jawab, dan upaya pemulihan, sesuai dengan prinsip-prinsip Situational Crisis Communication Theory (SCCT). Kolaborasi aktif dengan otoritas terkait seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI) juga terjadi. Langkah-langkah keamanan tambahan dan pemberian kompensasi menunjukkan komitmen BSI untuk melindungi nasabah. Keseluruhan, manajemen krisis BSI menciptakan fondasi kuat untuk memulihkan reputasi dan membangun kembali kepercayaan masyarakat dalam menghadapi dampak peretasan data.

Kata kunci: *Public relations*; *Krisis*; *SCCT*; *Perbankan*

Abstract

PT Bank Syariah Indonesia Tbk is a State-Owned Enterprise (SOE) engaged in Islamic banking currently facing a crisis, namely a data breach caused by a group of Lockbit 3.0 hackers. The aim of this research is to understand the crisis management conducted by BSI's public relations in the case of customer data breach by analyzing Crisis Management, including the factors causing the crisis, crisis mitigation strategies, and crisis resolution. This study uses the SCCT theory. According to Coombs & Holladay (2010), the Situational Crisis Communication Theory (SCCT) divides crisis response strategies into three main strategies: Deny Strategy, Diminishing Strategy, and Bolstering Strategy. This research uses a qualitative descriptive method. BSI's crisis management post-customer data breach proves to be responsive and effective. BSI identified the Lockbit ransomware attack and responded transparently through a press release that included apologies, responsibility, and recovery efforts, following the principles of SCCT. Active collaboration with relevant authorities such as the National Cyber and Crypto Agency (BSSN), the Financial Services Authority (OJK), and Bank Indonesia (BI) also took place. Additional security measures and compensation demonstrate BSI's commitment to protecting customers. Overall, BSI's crisis management creates a strong foundation for reputation recovery and rebuilding public trust in the face of the data breach impact.

Keywords: *Public relations, Crisis, SCCT, Banking*

PENDAHULUAN

Pada pertengahan 2023, BSI mengalami sebuah gangguan layanan *mobile banking* dan ATM BSI (Bank Syariah Indonesia) selama sepekan. Awalnya, BSI memberi penjelasan bahwa gangguan tersebut disebabkan oleh adanya pemiliharaan sistem sehingga layanan tidak dapat digunakan. Namun, fakta baru terungkap bahwa ganguan layanan disebabkan oleh sebuah serangan yang dinamakan dengan *ransomware* dari sekelompok *hacker*. Peretasan ini tidak hanya mengakibatkan semua layanan BSI berhenti namun ada pencurian data yang dilakukan. Data yang dicuri mencakup berbagai informasi pribadi dan keuangan, termasuk nama, alamat, nomor kartu, nomor telepon, dan transaksi nasabah, serta dokumen keuangan, dokumen hukum, dan kata sandi (*password*) untuk layanan internal dan eksternal yang digunakan oleh bank (Kompas.com., 2023).

Situasi menjadi kompleks ketika kelompok peretas yang dikenal dengan nama *LockBit 3.0* mengklaim bahwa mereka adalah pelaku di balik serangan tersebut. Mereka mengancam akan merilis data pribadi 1,5 TB yang mencakup informasi nasabah dan karyawan BSI jika tuntutan mereka tidak dipenuhi. Ancaman ini menciptakan kepanikan dan kekhawatiran di antara nasabah dan memaksa manajemen BSI untuk mengatasi masalah ini dengan serius. Meskipun, BSI bersikeras bahwa data dan dana nasabah aman namun publik tetap merasa cemas tentang potensi kebocoran data dan dampak serius yang dapat terjadi. Pasalnya, BSI

tidak menyampaikan pemberitahuan secara langsung kepada nasabah terkait data nasabah yang terikat dengan penyerangan siber yang berdambak pada peretasan data nasabah. Sementara BSI mengklaim gangguan hacker ini dengan berdalih adanya proses perbaikan sistem yang terganggu (Cnnindonesia.com., 2023).

Seperti hal yang terjadi di Aceh dengan pengguna terbesar bank BSI turut merasakan dampak dari gangguan yang terjadi, kekecewaan terjadi terhadap pengguna yang muncul akibat gangguan jaringan yang di sebabkan oleh serangan hacker dan layanan pelanggan yang kurang memuaskan. Hal ini, memicu terjadinya rencana perubahan kebijakan yang terjadi, seperti yang disampaikan oleh ketua DPR Aceh Saiful Bahri bahwa ia akan berkodinator dengan berbagai pihak untuk merevisi kebijakan Qanun Lembaga Keuangan Syariah (LKS) yang beroperasi di tanah rencong dan juga merencanakan agar perbankan konvensional bisa beroperasi di Aceh.

"Kami sudah bermusyawarah di lembaga kami menilai ini harus ditinjau ulang Qanun LKS supaya bank konvensional bisa tetap beroperasi di Aceh. Biarlah nanti masyarakat yang memilih mau bank syariah atau konvensional," kata Saiful kepada wartawan, (Detik.com, 2023).

Media memberikan perhatian besar pada isu peretasan data BSI, menjadikannya fokus utama dalam berita mereka. Spekulasi dan narasi negatif yang berkembang dalam liputan media dapat memperburuk citra BSI dan mengurangi kepercayaan masyarakat terhadap bank syariah, tetapi juga menciptakan tantangan serius bagi reputasi perbankan syariah di tingkat nasional. Dalam konteks ini, respons yang cepat dan efektif dari BSI menjadi kunci untuk memulihkan kepercayaan nasabah dan merestorasi citra perbankan syariah secara keseluruhan. Perbaikan sistem dan kebijakan perlindungan data yang lebih kuat juga menjadi langkah penting untuk mencegah terulangnya insiden serupa di masa depan. Media memiliki peran krusial dalam membentuk opini masyarakat terhadap suatu peristiwa, dan isu peretasan data yang melibatkan Bank Syariah Indonesia (BSI) menjadi sorotan utama. Spekulasi dan narasi negatif yang tersebar melalui liputan media dapat menciptakan dampak jangka panjang terhadap kepercayaan masyarakat terhadap perbankan syariah (Ritonga, 2018). Keberlanjutan pemberitaan ini dapat merugikan operasional BSI dan bahkan menciptakan tantangan serius bagi reputasi perbankan syariah di tingkat nasional. Berita mengenai serangan hacker terhadap BSI diberitakan secara dramatis, menciptakan narasi yang menekankan berbagai aspek serius dari peristiwa ini.

Freaming pemberitaan yang terjadi, memberikan kesan bahwa serangan ini bukan hanya mengancam satu lembaga keuangan, melainkan juga menjadi ujian berat bagi sektor perbankan Indonesia secara keseluruhan. Fokus media pada dampak luas dari serangan,

baik dari segi operasional BSI maupun reputasi perbankan syariah secara umum, meningkatkan kekhawatiran bahwa keamanan perbankan syariah secara menyeluruh terancam. Kurangnya informasi tentang langkah-langkah yang diambil oleh BSI untuk menangani situasi ini juga dapat meninggalkan kesan bahwa bank tidak mampu mengatasi masalah tersebut secara efektif. Spekulasi yang muncul tanpa sadar dapat menciptakan sentimen negatif di kalangan masyarakat.

Tabel 1. Pemberitaan media mengenai serangan hacker terhadap BSI

Media	Judul Artikel	Tanggal Rilis	Nilai
Kompas.tv.com	BSI Diretas Hacker Disebut Jadi Cobaan sekaligus Tantangan Perbankan Indonesia	17 Mei, 2023	(-)
Cnnindonesia.com	Dugaan Bank BSI Kena Serangan Ransomware, Pakar Ungkap Cirinya	10 Mei, 2023	(-)
Liputan6.com	BSI Diduga Kena Ransomware, Pakar: Antivirus Saja Belum Tentu Bisa Melawan	10 Mei, 2023	(-)
Bisnis.tempo.co	BSI Kena Serangan Ransomware, Nasabah Mengaku Rugi Ratusan Juta	13 Mei, 2023	(-)

Sumber : Media Online, 2023

Dari data pemberitaan di atas, ini menunjukkan bahwa kebocoran data pribadi nasabah tentu sangat berdampak besar bagi nasabah maupun bank BSI milik BUMN ini. Selain, menimbulkan ketidaknyamanan bagi nasabah, serangan hacker terhadap bank BSI juga dapat berdampak kerugian citra dan reputasi bagi bank BSI. Dalam hal ini, manajemen krisis harus dilakukan jika terjadi krisis. Nilai-nilai utama seperti kesadaran akan terjadinya krisis, ketepatan, kecepatan, dan tanggung jawab senantiasa menjadi pedoman bagi semua kegiatan dan keputusan yang diambil oleh otoritas pemerintah dan terutama perusahaan

dalam menangani keadaan krisis yang terjadi selama menggunakan manajemen krisis (Yuliana, 2022).

Krisis digambarkan sebagai suatu peristiwa yang merupakan kejutan dimana tidak ada satupun organisasi atau perusahaan yang berharap hal tersebut terjadi atasnya. Menurut Michael Regester dan Judy Larkin (2008) krisis merupakan situasi yang membuat perusahaan menjadi subjek pembicaraan kalangan luas, yang berpotensi untuk ridak disukai, mendapat sorotan dari berbagai media baik nasional maupun internasional dan berbagai kelompok lainya (seperti konsumen, pemegang saham, karyawan serta keluarganya, poitisi, serikat perdagangan, kelompok lingkungan lingkungan hidup) yang disebabkan satu alasan tertentu memiliki ketertarikan terhadap segala aktifitas yang dilaksanakan oleh perusahaan (Puspitasari, 2016).

Peran public relations sangat dibutuhkan dalam penanganan manajemen krisis dalam suatu perusahaan. Dalam lingkupnya pelaksanaan komunikasi saat kriris merupakan syarat yang tidak boleh diabaikan oleh suatu perusahaan yang mengalami krisis. Dengan demikian, Manajemen krisis dibutuhkan dalam suatu Perusahaan untuk selalu mencegah terjadinya krisis yang meluas dan mengubah presepsi publik kepada perusahaan kearah yang lebih baik lagi. Dalam pelaksanaanya, public relations harus berjalan berdasarkan konsep-konsep manajemen dalam setiap perusahaan untuk mempermudah aktifitasnya, terlebih apabila perusahaan sedang mengalami krisis. Keberadaan public relation akan sangat diperlukan dalam penanganan krisis karena public relations mengarah pada sistem pendekatan manajerial prosesnya berupa *planning* (perencanaan), *organizing* (pengorganisasian), *actuating* (penggiatan), dan *controlling* (pengawasan). Semua prosesnya bertujuan untuk mempertahankan citra baik perusahaan serta berperan untuk mewujudkan situasi yang kondusif setelah mengalami *krisis* baik terhadap pihak internal perusahaan ataupun eksternal perusahaan (*Stakeholders)* (Maulida *et al,* 2022).

Penelitian ini akan membahas permasalahan tentang manajemen krisis yang dilakukan public relations BSI dalam krisis pasca terjadinya peretasan data nasabah. Kasus ini tentu berkaitan dengan citra yang dimiliki oleh BSI. Secara, BSI merupakan harapan bagi pemerintah dan para pelaku bisnis dalam dunia perbankan dalam meningkatkan pasar keuangan syariah Indonesia di mata dunia. Tentunya, dengan adanya kasus peretasan data yang di sebabkan sekelompok hacker bernama *LockBit 3.0* dapat berdampak besar terhadap citra yang dimiliki BSI. Terlebih, BSI memiliki visi menjadi menjadi bank syariah berskala dunia, yaitu target untuk masuk dalam peringkat 10 besar bank syariah dunia dengan nilai kapitalisasi besar pada 2025 (Suhaimi, 2021).

Teori yang digunakan dalam penelitian ini adalah teori *Situasional Crisis Communication Theory* (SCCT). *Situational Crisis Communication Theory* atau SCCT mengatur strategi sigap menangani krisis dengan menentukan apa yang dimaksud dari strategi tersebut adalah untuk mengubah persepsi tentang krisis atau perusahaan yang sedang dilanda krisis (Coombs & Holladay, 2010). Menurut Coombs & Holladay (2010) *Situational Crisis Communication Theory (SCCT)* membagi strategi respon krisis menjadi tiga strategi utama, yaitu : *Deny Strategy* (Strategi Penolakan) merupakan upaya untuk membuktikan bahwa suatu perusahaan atau organisasi tidak bertanggung jawab atas krisis tersebut, Melainkan orang lain harus bertanggung jawab atas kejadian itu; *Diminish Strategy* (Strategi Mengurangi) merupakan suatu strategi yang bertujuan untuk meminimalkan tanggung jawab serta mengurangi keseriusan dalam menangani krisis; *Bolstering Strategy* (Memperkuat Strategi) Merupakan usaha mengingatkan publik dengan menyampaikan pemahaman bahwa suatu perusahaan atau organisasi diisi dengan individu-individu yang memiliki kualitas tinggi dalam menjalankan tugas sehari-hari sehingga resiko terjadinya krisis menjadi minim.

Penelitian terdahulu yang dilakukan Yulianti & Boer (2020) menggunakan teori SCCT mengenai "Manajemen krisis public relations dalam menangani penolakan imunisasi measles rubella" menjelaskan bahwa penanganan krisis yang dilakukan public relations Kementerian Kesehatan melibatkan komunikasi dan kerja sama dengan para stakeholder, penyebaran release melalui website, berkomunikasi dengan Pemerintahan daerah, Dinas Kesehatan daerah, serta memanfaatkan media tradisional dan digital. Selanjutnya, penelitian sejenis yang dilakukan Suryani & Sagiyanto (2018) menjelaskan bahwa manajemen krisis lewat program "reimagining Blue Bird." Program ini disuarakan melalui iklan kampanye Blue Bird "Berbenah Untuk Berubah" di YouTube dan berhasil mendapat simpati dari publik yang akhirnya dapat membangun opini publik positif sehingga berdampak terhadap reputasi Blue Bird.

Berdasarkan penjelasan terkait permasalahan, latar belakang dan pemaparan *literature review* sebelumnya. Penelitian ini memiliki fokus terhadap "Manajeman Krisis PT. BSI Tbk Pasca Peretasan Data Nasabah" yang diperdalam menggunakan teori *Situational Communication Crisis Theory* (SCCT).

METODE PENELITIAN

Jenis penelitian yang digunakan dalam penelitian ini adalah penelitian kualitatif, Penelitian kualitatif ini bertujuan untuk memahami secara mendalam terkait krisis yang menimpa Bank Syariah Indonesia. Penelitian ini juga menggunakan teknik analisis data

menggunakan studi literatur (*Literature Review*), yaitu istilah yang digunakan untuk merujuk pada suatu metode penelitian atau pengembangan tertentu yang melibatkan pengumpulan dan evaluasi studi-studi terkait pada fokus topik tertentu (Triandini, Jayanatha, Indrawan, Werla Putra, & Iswara, 2019). Selain itu, penelitian ini juga melakukan wawancara pada salah satu dosen ekonomi Universitas Muhammadiyah Jakarta, yaitu Sampor Ali, M.M., S.Hum., S.Hum., untuk memberikan analisis yang jauh lebih dalam berkaitan manajemen krisis yang dilakukan dalam kasus peretasan data di Bank BSI. Fokus serta batasan dari penelitian ini adalah manajeman krisis BSI terkait peretasan data nasabah. Teknik pengumpulan data terdiri dari dua teknik yaitu data primer dan data sekunder. Untuk penelitian ini data primer yang dipilih adalah pemberitaan terkait peretasan data nasabah Bank Syariah Indonesia pada media elektronik dari tanggal 10-18 Mei 2023. Data sekunder pada penelitian ini diambil dari jurnal, literature, serta artikel internet terkait permasalahan penelitian.

HASIL DAN PEMBAHASAN

Peristiwa kronologi peretasan data nasabah Bank Syariah Indonesia (BSI) yang diuraikan oleh pakar keamanan siber Alfons Tanujaya, terungkap bahwa BSI menjadi sasaran serangan ransomware, khususnya jenis Lockbit. Alfons memaparkan detail peristiwa mulai dari penemuan kebocoran data sebesar 1,5 TB hingga analisis waktu pencurian yang menunjukkan serangan yang terorganisir yang dijelaskan sebagai berikut:

1. Identifikasi Jenis *Ransomware*

   Pada awalnya, Alfons Tanujaya mengidentifikasi bahwa BSI menjadi korban ransomware, dengan jenis ransomware yang disebut Lockbit. Ransomware adalah jenis serangan siber di mana peretas mengenkripsi data korban dan meminta tebusan agar data tersebut dapat dikembalikan.
2. Penemuan Kebocoran Data

   Alfons Tanujaya membeberkan bahwa kelompok ransomware Lockbit tidak hanya mengancam, tetapi juga telah berhasil mencuri dan mengenkripsi data sebesar 1,5 TB milik BSI. Proses pencurian data yang sebesar itu membutuhkan waktu yang sangat panjang, mengindikasikan bahwa peretasan ini merupakan serangan yang terorganisir dan cermat.
3. Tanggal Kejadian Sebelum 8 Mei 2023

   Alfons menyatakan bahwa kejadian peretasan kemungkinan besar terjadi sebelum tanggal 8 Mei 2023. Pada tanggal tersebut, terjadi error pada aplikasi BSI Mobile yang membuatnya tidak dapat digunakan.
4. Analisis Waktu Pencurian Data

Pakar keamanan siber ini memberikan perhitungan terkait waktu pencurian data. Dengan asumsi pencurian dilakukan secara kontinu selama 24 jam dengan kecepatan transfer data 25 Mbps, diperkirakan waktu yang dibutuhkan untuk mencuri dan mengenkripsi data sebesar 1,5 TB adalah 6 hari. Namun, Alfons juga mencatat bahwa peretasan dilakukan dengan hati-hati untuk menghindari kecurigaan, yang dapat memperpanjang waktu pencurian menjadi 12 hari.

5. Periode Libur Lebaran

   Dengan merinci waktu peretasan sebelum tanggal 8 Mei, Alfons menyimpulkan bahwa kemungkinan besar aksi peretasan telah dimulai sejak libur Lebaran. Periode libur ini dapat dijadikan peluang bagi peretas untuk menjalankan aksi mereka tanpa terdeteksi lebih cepat.

6. Dampak Kebocoran Data

   Alfons juga menggambarkan dampak dari kebocoran data tersebut. Salah satu dampaknya adalah ekspos kondisi keuangan nasabah yang memiliki saldo tidak wajar. Selain itu, data sensitif seperti kredensial m-banking, internet banking, dan email berpotensi bocor, mengancam keamanan informasi pribadi nasabah dan karyawan.

7. Rekomendasi dan Mitigasi

   Sebagai respons terhadap kebocoran data, Alfons memberikan rekomendasi kepada pemilik akun BSI untuk segera mengganti semua kredensial m-banking, internet banking, dan pin ATM sebagai tindakan mitigasi.

8. Peringatan kepada Perusahaan Besar

   Alfons juga memperingatkan perusahaan besar untuk selalu waspada terhadap risiko kebocoran data. Ia menekankan pentingnya perusahaan bersikap selayaknya perusahaan besar dengan menghitung risiko dan biaya sebelum mengambil keputusan, sebagai langkah preventif.

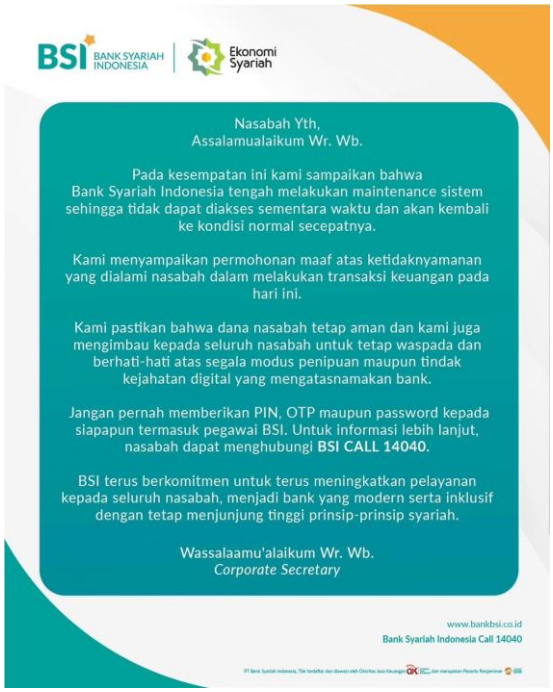
Menanggapi hal tersebut, penanganan terhadap kebocoran data yang dilakukan oleh BSI melibatkan serangkaian langkah untuk memastikan keamanan dan kenyamanan nasabah. Pertama, BSI menyatakan bahwa data dan dana nasabah aman, serta dapat bertransaksi dengan aman. Perusahaan berkomitmen untuk bekerja sama dengan otoritas terkait, seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI) dalam menanggapi isu kebocoran data ini.

Kedua, BSI melakukan investigasi internal dan terus berkoordinasi dengan berbagai pihak terkait. Proses pengecekan dan tindak lanjut terhadap keseluruhan sistem dilakukan, termasuk mitigasi jangka panjang untuk mencegah terulangnya serangan serupa di masa

depan. Gangguan sistem yang terjadi sejak 8 Mei 2023 telah diatasi secara bertahap, memungkinkan nasabah untuk kembali melakukan transaksi keuangan dan pembayaran.

Ketiga, BSI juga mengambil langkah-langkah keamanan ekstra, seperti melakukan asesmen terhadap serangan, pemulihan, audit, dan mitigasi agar gangguan serupa tidak terulang. Peringatan disampaikan kepada nasabah untuk tidak memberikan PIN, OTP, atau password kepada siapa pun, termasuk pegawai BSI, sebagai langkah pencegahan. Keempat, BSI menyampaikan permohonan maaf atas ketidaknyamanan yang dialami nasabah selama proses normalisasi layanan. Komitmen untuk menjaga keamanan data dan memberikan pelayanan yang optimal bagi nasabah menjadi fokus utama dalam penanganan situasi ini.

Sementara itu, berdasarkan hasil analisis pemberitaan yang peneliti lakukan, dalam merespon krisis yang dihadapi oleh Bank Syariah Indonesia (BSI), *Deny strategies* dilakukan oleh BSI dengan menganggap bahwa mereka memang tidak sedang menghadapi krisis, tetapi ada rumor bahwa BSI sedang menghadapi sebuah krisis/masalah serius. Dalam strategi ini, bentuk pesan atau pernyataan bisa berupa: *denial*. Menurut Benoit (2015) penolakan (*denial*) , strategi untuk menolak semua tuduhan yang ditujukan kepada suatu perusahaan melalui penolakan sederhana atau mengalihkan kesalahan. BSI menyangkal adanya sesuatu yang tidak beres; Berikut pernyataan yang dikeluarkan BSI dalam postingan Instagram resminya :



Gambar 1. Ucapan permintaan maaf yang dikeluarkan oleh pihak BSI

Sumber: @banksyariahindonesia

Melalui laman instagram resmi BSI, Corporate Secretary Bank Syariah Indonesia (BSI) memberikan sebuah pernyataan yang menjadi tanggapan terhadap krisis yang melibatkan peretasan data nasabah BSI. Dalam pernyataan tersebut, Corporate Secretary menegaskan

bahwa BSI mengadopsi sikap denial atau sanggahan terkait peristiwa yang menimpa BSI. Pernyataan ini ditujukan untuk memberikan respon terhadap situasi yang sedang terjadi pada BSI.

Denial atau penyangkalan, sebagai mekanisme pertahanan diri yang diadopsi oleh Bank Syariah Indonesia (BSI), merujuk pada sikap menolak atau menyangkal untuk mengakui fakta terjadinya suatu peretasan. Denial ini mencerminkan strategi komunikasi yang diterapkan oleh BSI, di mana lembaga tersebut berusaha untuk mengubah atau menyangkal interpretasi fakta yang beredar di masyarakat terkait dengan peretasan data. Dengan kata lain, BSI secara sadar dan aktif menolak untuk mengakui kebenaran dari peristiwa tersebut.

Dalam mengadopsi *Deny Strategy*, Bank Syariah Indonesia (BSI) berusaha untuk memanfaatkan komunikasi yang hati-hati, penjelasan yang terperinci, atau bahkan retorika yang dapat merubah persepsi publik terkait peretasan yang terjadi pada BSI. Meskipun dapat memberikan keuntungan dalam mengelola citra, tetapi *Deny Strategy* juga dapat menimbulkan risiko jika terbukti informasi yang diberikan tidak sesuai dengan fakta kepada para nasabah terkait persoalan peretasan data nasabah.

Dalam menghadapi permasalahan serius terkait gangguan layanan yang terjadi pada Bank Syariah Indonesia (BSI), PT BSI menjalankan strategi komunikasi krisis yang mencerminkan prinsip-prinsip Situational Crisis Communication Theory (SCCT) dan telah memberikan respon terhadap krisis yang terjadi. Sebagai langkah konkret dalam menanggapi krisis, BSI memutuskan untuk menerbitkan *press release*. Keputusan ini sejalan dengan prinsip-prinsip SCCT yang menekankan pentingnya komunikasi terbuka dan jelas selama krisis. *Press release* merupakan saluran efektif untuk menyampaikan informasi resmi, menjelaskan kondisi saat ini, dan memberikan langkah-langkah yang akan diambil untuk mengatasi masalah tersebut.

BSI BANK SYARIAH INDONESIA

PRESS RELEASE

Dirut BSI : Kami Mohon Maaf dan Sedang Berusaha Pulihkan Layanan

Jakarta, 10 Mei 2023 – PT Bank Syariah Indonesia Tbk. (BSI) menyampaikan permohonan maaf atas kendala yang dialami nasabah dalam mengakses layanan BSI sekaligus menegaskan komitmen untuk menjaga keamanan dana dan data milik nasabah.

Direktur Utama BSI Hery Gunardi menuturkan bahwa pihaknya terus melakukan proses normalisasi dengan fokus utama untuk menjaga dana dan data nasabah tetap aman, dan hingga saat ini proses normalisasi layanan telah dilakukan dengan baik.

"Atas nama Bank Syariah Indonesia, kami menyampaikan permohonan maaf atas ketidaknyamanan nasabah karena adanya kendala dalam mengakses layanan BSI pada 8 Mei 2023. Proses normalisasi layanan Bank Syariah Indonesia telah kami lakukan, dengan prioritas utama untuk meyakinkan dana dan data nasabah tetap aman di Bank Syariah Indonesia," ujar Hery dalam keterangannya di Jakarta, Rabu (10/5/2023).

Pada Selasa (9/5/2023), BSI telah berhasil melakukan normalisasi layanan pada jaringan ATM dan kantor cabang. Pada hari tersebut, lanjutnya, nasabah telah bisa melakukan transaksi di jaringan cabang dan ATM BSI yang tersebar di seluruh Indonesia. Masih pada hari yang sama, Selasa (9/5/2023) malam, secara bertahap layanan BSI Mobile juga sudah dapat diakses oleh nasabah dengan fitur-fitur basic.

Kemudian pada hari ini, Rabu (10/5/2023) pukul 14.00 WIB, Perseroan tengah melakukan monitoring dan proses normalisasi transaksi yang berdampak pada layanan BSI tidak bisa diakses sementara waktu yakni layanan di cabang, akses BSI Mobile maupun ATM di seluruh Indonesia. Kami akan terus memberikan informasi terkini sehingga nasabah dapat bertransaksi dengan normal.

Adapun terkait dengan adanya serangan cyber, lanjutnya, pada dasarnya BSI akan melakukan penelusuran atas hal tersebut.

"Hal tersebut perlu pembuktian lebih lanjut melalui audit dan digital forensik. Kami terus berkoordinasi dengan berbagai pihak, baik itu regulator maupun pemerintah," tutur Hery.

Hery pun menegaskan komitmen BSI sebagai institusi perbankan untuk terus memperkuat pertahanan dan keamanan cyber, terutama demi kepentingan nasabah.

Pihaknya juga tidak henti mengingatkan nasabah untuk terus menjaga kewaspadaan dan berhati-hati terhadap berbagai bentuk modus penipuan serta kejahatan digital yang mengatasnamakan Bank Syariah Indonesia.

"Sekali lagi kami mohon maaf atas ketidaknyamanan ini dan terima kasih atas dukungan dan kepercayaan yang diberikan kepada BSI," tutupnya.

Mengenai Bank Syariah Indonesia

PT Bank Syariah Indonesia Tbk ("Bank Syariah Indonesia") adalah bank hasil penggabungan dari tiga bank Syariah milik BUMN yakni PT Bank Syariah Mandiri, PT Bank BNI Syariah, dan PT Bank BRIsyariah Tbk. yang mulai beroperasi pada 1 Februari 2021. Penggabungan ini menyatukan kekuatan ketiga bank syariah tersebut dan bertujuan untuk mengoptimalkan potensi keuangan dan ekonomi syariah Indonesia yang besar. Didukung sinergi dengan perusahaan induk (Mandiri, BNI, BRI) serta komitmen pemerintah melalui Kementerian BUMN, Bank Syariah Indonesia memiliki visi untuk menjadi salah satu dari 10 bank Syariah terbesar di dunia dari sisi kapitalisasi pasar dalam 5 tahun ke depan.

Gambar 2. *Press release* yang dikeluarkan oleh pihak BSI

Sumber : bankbsi.co.id

Dalam *press release* yang diterbitkan oleh PT Bank Syariah Indonesia (BSI), Direktur Utama BSI, Hery Gunardi, dengan tulus menyampaikan permohonan maaf kepada seluruh nasabah atas ketidaknyamanan yang mereka alami akibat kendala dalam mengakses layanan BSI pada tanggal 08 Mei 2023. Hery Gunardi menekankan bahwa kenyamanan dan keamanan nasabah adalah prioritas utama perusahaan, dan gangguan layanan ini sangat disayangkan.

Untuk mengatasi permasalahan ini, pihak BSI telah mengambil langkah-langkah konkret. Direktur Utama BSI menyampaikan bahwa perusahaan telah segera melakukan investigasi menyeluruh terkait dengan gangguan layanan tersebut. Meskipun ada kemungkinan terjadinya serangan cyber, pihak BSI tidak mengabaikan kemungkinan faktor lain yang dapat menjadi penyebab. Investigasi ini dilakukan dengan itikad baik untuk memahami sumber permasalahan dan mencegah terulangnya kejadian serupa di masa depan. Dalam keseluruhan keterangannya, Direktur Utama BSI mencerminkan sikap transparan dan bertanggung jawab. Ia menegaskan bahwa BSI akan terus memberikan informasi yang akurat dan terkini kepada nasabah serta masyarakat seiring berjalannya investigasi dan upaya pemulihan.

Dengan adanya *press release* yang diterbitkan lewat website resmi BSI, ia menetapkan dirinya dalam cluster Situational Crisis Communication Theory (SCCT) yang dimana dalam merespon krisis permasalahan gangguan layanan pada sistem BSI. Timothy Comb dalam Situational Crisis Communication Theory (SCCT, 2007), mengatakan, salah satu *Crisis Response Strategy* adalah *Rebuild Crisis Response* dimana perusahaan harus menyatakan permintaan maaf (apology) dan bahwa perusahaan bertanggung jawab penuh atas kondisi yang terjadi untuk mengembangkan komunikasi institusi dengan publik agar berjalan dengan baik untuk mewujudkan goodwill dan mutual understanding terhadap publik, Dengan ini BSI menaruh harapan dengan adanya strategi rebuild ini bisa membangun kepercayaan kembali Masyarakat terhadap permasalahan ini. Pihak Bank Syariah Indonesia (BSI) tidak hanya mengandalkan penerbitan press release sebagai respons terhadap permasalahan peretasan yang dilakukan oleh kelompok cyber ransomware lockbit 3.0. Mereka juga mengambil langkah konkrit dengan memberikan kompensasi kepada para nasabah atau pihak yang mengalami kerugian akibat insiden tersebut.

Dr. Pratama Persadha, yang menjabat sebagai Chairman Lembaga Riset Keamanan Siber dan Komunikasi CISSReC (Communication and Information System Security Research Center), menyatakan bahwa BSI telah berkomitmen untuk memberikan kompensasi kepada

nasabah yang mengalami kerugian terkait peretasan data nasabah (BBC, 2023). Menurutnya, berdasarkan pasal 83 ayat 5, BSI diwajibkan memberikan kompensasi sebesar 20 juta euro atau setara dengan 320 miliar rupiah kepada para nasabah yang dirugikan dalam permasalahan ini, sesuai dengan ketentuan yang berlaku.

Selain itu, dikaitkan dengan toeri SCCT dapat dijelaskan secara lebih sistematis. Persepsi publik terhadap krisis ini mencapai tingkat yang tinggi, seiring dengan seriusnya peretasan data nasabah yang berpotensi menimbulkan kerugian finansial dan reputasi. Kendati demikian, kontrol yang dimiliki oleh BSI atas krisis ini terbilang rendah, mengingat peretasan dilakukan oleh pihak eksternal yang tidak dikenal dan di luar kendali perusahaan. Kepentingan publik terhadap krisis ini juga sangat tinggi, mengingat data pribadi nasabah menjadi taruhannya.

Dalam menanggapi krisis ini, BSI memilih menerapkan strategi komunikasi yang dapat dikategorikan sebagai *rebuild crisis response*. Melalui pendekatan ini, BSI secara terbuka menyampaikan permintaan maaf kepada nasabah, mengakui ketidaknyamanan yang mereka alami, dan menegaskan tanggung jawab penuh atas kejadian peretasan tersebut. Langkah-langkah pemulihan yang diambil oleh BSI mencakup investigasi menyeluruh, peningkatan keamanan sistem informasi, dan pemberian kompensasi kepada nasabah yang mengalami kerugian. Tindakan-tindakan ini bukan hanya sekadar respons, melainkan upaya konkret untuk memulihkan layanan dan mencegah terulangnya kejadian serupa di masa depan.

Selain menerapkan strategi *rebuild crisis response*, BSI juga mengambil langkah-langkah tambahan. Mereka menjalin komunikasi terbuka dan transparan dengan publik melalui serangkaian press release yang memberikan informasi terkini terkait penanganan krisis. Kerja sama aktif dengan lembaga terkait, seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI), menandakan upaya BSI untuk memperoleh dukungan dan masukan yang diperlukan dalam mengatasi krisis ini. Keseluruhan, langkah-langkah ini menciptakan landasan yang kuat untuk memulihkan reputasi dan membangun kembali kepercayaan masyarakat, menunjukkan komitmen BSI dalam menangani krisis dengan serius dan efektif.

Pernyataan Sampor Ali, M.M. S.Hum., S.Hum., dosen program studi Manajemen Universitas Muhammadiyah Jakarta turut berkomentar terkait kasus ini. penanganan krisis BSI dianggap sudah tepat namun masih kurang, hal ini menunjukkanbahwa meskipun langkah-langkah responsif telah diambil, masih ada kebutuhan untuk mendalam dan mengevaluasi faktor-faktor yang memengaruhi tingkat kepercayaan nasabah. Evaluasi lebih

lanjut dapat melibatkan analisis mengenai transparansi informasi, integritas kebijakan keamanan, dan komunikasi yang efektif untuk membangun kembali kepercayaan nasabah.

Penggantian beberapa direksi, terutama di bidang teknologi dan risiko, mencerminkan respons manajemen BSI yang tegas terhadap kejadian peretasan. Langkah ini dapat diartikan sebagai usaha konkret untuk meningkatkan manajemen risiko dan keamanan teknologi perbankan. Evaluasi mendalam terhadap kebijakan dan praktik keamanan IT, serta implementasi teknologi keamanan yang mutakhir, mungkin perlu diperkuat untuk memastikan kehandalan sistem di masa mendatang.

Tindakan memberikan keringanan kepada nasabah yang terkena gangguan, seperti izin transfer dengan nominal 0 rupiah, adalah langkah proaktif yang dapat meredakan dampak negatif pada nasabah yang mungkin mengalami kesulitan. Respons yang tanggap seperti ini adalah strategi untuk memperkuat hubungan perbankan dan membangun kembali kepercayaan masyarakat. Evaluasi lebih lanjut dapat dilakukan untuk memahami sejauh mana tindakan ini memberikan manfaat konkret kepada nasabah dan apakah langkah serupa perlu diterapkan pada tingkat yang lebih luas dalam menangani krisis serupa di masa depan.

Dengan melakukan investigasi menyeluruh terhadap akar penyebab peretasan, BSI dapat mengidentifikasi potensi celah keamanan dan memperkuat pertahanan sistem mereka. Selanjutnya, peningkatan keamanan sistem informasi menjadi fokus utama dalam mencegah serangan serupa di masa depan. Keterlibatan pihak berwenang dan pemangku kepentingan eksternal juga berperan penting dalam proses perbaikan ini, memastikan adanya pertanggungjawaban yang komprehensif dan meminimalkan risiko krisis serupa. Dengan menggabungkan upaya pemulihan, komunikasi terbuka, dan perbaikan struktural, BSI secara holistik merespon krisis peretasan data dengan mengintegrasikan aspek teknis dan komunikatif untuk membangun fondasi yang kuat dan mengembalikan kepercayaan publik.

SIMPULAN

Manajemen krisis PT. Bank Syariah Indonesia (BSI) Tbk pasca peretasan data nasabah dapat dianggap sebagai langkah-langkah responsif dan efektif dalam menghadapi situasi yang mengancam keamanan dan reputasi perusahaan. BSI secara cermat mengidentifikasi serangan ransomware Lockbit dan dengan cepat merespons dengan transparan melalui press release yang diterbitkan. Respons tersebut mencakup permintaan maaf, tanggung jawab, dan upaya pemulihan, yang sesuai dengan prinsip-prinsip *Situational Crisis Communication Theory* (SCCT). BSI juga terlibat aktif dengan otoritas terkait seperti Badan

Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI) untuk menangani isu kebocoran data. Penerapan langkah-langkah keamanan tambahan dan pemberian kompensasi kepada nasabah yang dirugikan menunjukkan komitmen BSI untuk melindungi keamanan dan kenyamanan nasabahnya. Keseluruhan, manajemen krisis PT. BSI Tbk pasca peretasan data nasabah menciptakan dasar yang solid untuk memulihkan reputasi perusahaan dan membangun kembali kepercayaan masyarakat.

DAFTAR PUSTAKA

Benoit, W. L. (2015). *Accounts, Excuses, and Apologies, Second Edition: Image Repair Theory and Research*. New York: State University of New York Press.

Cnnindonesia.com. (2023). Lockbit 3.0 Diduga Curi Data dan Password 15 Juta Data Nasabah BSI. *Cnnindonesia.Com.* Diakses melalui dari https://www.cnnindonesia.com/ekonomi/20230513102703-92-949058/lockbit-30-diduga-curi-data-dan-password-15-juta-nasabah-bsi

Coombs, T., & Holladay, S. (2010). *The Handbook of Crisis Communication*. UK: Blackwell Publishing.

Detik.com. (2023). Revisi Qanun LKS Mencuat, DPRA Ingin Bank Konvensional Beroperasi Lagi di Aceh. *Detik.Com*. Diakses melalui https://www.detik.com/sumut/bisnis/d-6715825/revisi-qanun-lks-mencuat-dpra-ingin-bank-konvensional-beroperasi-lagi-di-aceh

Kompas.com. (2023). "Hacker" Ancam Bocorkan Data 15 Juta Nasabah dan Karyawan BSI yang dicuri, Dirut: Keamanan Sistem IT Diperkuat. *Kompas.Com.* Diakses melalui https://money.kompas.com/read/2023/05/13/170000926/-hacker-ancam-bocorkan-data-15-juta-nasabah-dan-karyawan-bsi-yang-dicuri-dirut?page=all

Puspitasari. (2016). *Komunikasi Krisis : Strategi Mengelola Dan Memenangkan Citra Di Mata Publik*. Jakarta: Libri.

Ritonga, E. Y. (2018). Teori Agenda Setting dalam Ilmu Komunikasi. *JURNAL SIMBOLIKA: Research and Learning in Communication Study*, *4*(1), 32. https://doi.org/10.31289/simbollika.v4i1.1460

Suhaimi, A. (2021). Studi Manajeman Risiko Pada Bank Syariah Indonesia (Bsi). *Jurnal Manajemen Risiko*, *2*(I), 73–78. https://doi.org/10.33541/mr.v2ii.3438

Suryani, I., & Sagiyanto, A. (2018). Strategi Manajemen Krisis Public Relations PT Blue Bird Group. *Communication*, *9*(1), 103. https://doi.org/10.36080/comm.v9i1.624

Triandini, E., Jayanatha, S., Indrawan, A., Werla Putra, G., & Iswara, B. (2019). Metode Systematic Literature Review untuk Identifikasi Platform dan Metode Pengembangan

Sistem Informasi di Indonesia. *Indonesian Journal of Information Systems*, *1*(2), 63. https://doi.org/10.24002/ijis.v1i2.1916

Yuliana, L. (2022). Pemanfaatan Manajemen Krisis Terhadap Brand Awareness. *Widya Cipta: Jurnal Sekretari Dan Manajemen*, *6*(2), 95–101. https://doi.org/10.31294/widyacipta.v6i2.12633

Yulianti, W., & Boer, R. F. (2020). Manajemen krisis public relations dalam menangani penolakan imunisasi measles rubella. *PRofesi Humas Jurnal Ilmiah Ilmu Hubungan Masyarakat*, *4*(2), 290. https://doi.org/10.24198/prh.v4i2.23700