COSTING: Journal of Economic, Business and Accounting
Volume 8 Nomor 4, Tahun 2025
e-ISSN : 2597-5234

THE IMPACT OF CYBER ATTACKS ON THE PROFITABILITY AND DIVIDEND POLICY OF INDONESIAN SHARIA BANKS

DAMPAK SERANGAN SIBER TERHADAP PROFITABILITAS DAN KEBIJAKAN DIVIDEN BANK SYARIAH INDONESIA

Heranita Nur Afifah[1], Khoirul Fatah[2]
Universitas Muhammadiyah Pekajangan Pekalongan, Kota Pekalongan[1,2]
nitaafifah03@gmail.com[1], fatahirul@gmail.com[2]

ABSTRACT

The purpose of this study is to examine how cyberattacks impact dividend policy and profitability of PT Bank Syariah Indonesia Tbk and the moderating role of company size in this regard. Financial and capital market data from January to August 2023 were used for a quantitative approach, employing event studies and multiple linear regression. The results show that Bank Syariah Indonesia experienced an increase in Return on Assets (ROA) after the cyberattack, although a cyberattack is theoretically expected to decrease profitability. This indicates that the bank has the ability to adapt and improve its operational efficiency. Company size is evident, reducing the impact of cyberattacks on profitability, but not on dividend policy. However, the Dividend Payout Ratio (DPR) did not experience significant changes, indicating that the company's dividend approach remained the same. These results suggest that larger companies are more resilient to cyber threats and can maintain market confidence by adhering to consistent policies. This study adds to the research on cyber risk management and financial policy in Islamic banking.

Keywords*: Cyberattack, Profitability, Dividend, Firm Size, Islamic Banking.*

ABSTRAK

Tujuan dari penelitian ini adalah untuk mempelajari bagaimana serangan siber berdampak pada kebijakan dividen dan profitabilitas PT Bank Syariah Indonesia Tbk dan bagaimana peran moderasi ukuran perusahaan dalam hal ini. Data keuangan dan pasar modal dari Januari hingga Agustus 2023 digunakan untuk pendekatan kuantitatif, yang menggunakan studi peristiwa dan regresi linier berganda. Hasil penelitian menunjukkan bahwa Bank Syariah Indonesia mengalami peningkatan *Return on Assets* (ROA) setelah serangan siber, meskipun secara teoritis serangan siber diharapkan menurunkan profitabilitas. Ini menunjukkan bahwa bank memiliki kemampuan untuk beradaptasi dan meningkatkan efisiensi operasionalnya. Terbukti bahwa ukuran perusahaan mengurangi dampak serangan siber terhadap profitabilitas, tetapi tidak terhadap kebijakan dividen. Namun, *Dividend Payout Ratio* (DPR) tidak mengalami perubahan yang signifikan, menunjukkan bahwa pendekatan dividen perusahaan tetap sama. Hasil ini menunjukkan bahwa perusahaan besar lebih tahan terhadap ancaman siber dan dapat mempertahankan kepercayaan pasar dengan mengikuti kebijakan yang konsisten. Studi ini menambah penelitian tentang manajemen risiko siber dan kebijakan keuangan dalam perbankan syariah.

Kata Kunci : Serangan Siber, Profitabilitas, Dividen, Ukuran Perusahaan, Perbankan Syariah.

PENDAHULUAN

Industri perbankan yang mengalami transformasi digital telah menghasilkan paradoks keamanan yang signifikan di mana peningkatan layanan digital sebanding dengan peningkatan risiko keamanan siber. Fenomena ini menjadi semakin penting ketika melibatkan perbankan syariah, yang beroperasi berdasarkan prinsip kepercayaan dan transparansi. Menurut data Statista (2024), insiden siber di bidang keuangan di seluruh dunia meningkat drastis dari 1.829 kasus pada 2022 menjadi 3.348 kasus pada 2023, dan pelanggaran data meningkat dari 690 menjadi 1.115 pada periode yang sama. Badan Siber dan Sandi Negara (BSSN) mencatat 347 dugaan insiden siber di Indonesia sepanjang tahun 2023, 38 di antaranya terjadi di sektor keuangan, dengan 165 ribu data keuangan tersebar di darknet.

Serangan *ransomware LockBit 3.0* terhadap PT Bank Syariah Indonesia Tbk (BSI) pada Mei 2023 adalah contoh nyata dari ancaman siber yang memiliki kemampuan untuk mengganggu stabilitas keuangan perbankan syariah. Ini menyebabkan gangguan operasi selama empat hari, kebocoran 1,5 *terabyte* data pelanggan, dan kerugian diperkirakan sebesar Rp 1,4 triliun. Dampak tersebut tidak hanya berdampak pada aspek operasional, tetapi juga menyebabkan fluktuasi harga saham BRIS yang signifikan selama periode setelah serangan.

Penelitian kontemporer menunjukkan bahwa serangan siber berdampak negatif pada kinerja keuangan bisnis. (Romanosky et al., 2019) menunjukkan bahwa serangan siber dan harga saham perusahaan publik berkorelasi negatif, terutama dalam kasus kebocoran data massal. (Gordon et al., 2021) menemukan bahwa perusahaan besar menjadi sasaran utama peretas, tetapi mereka memiliki kemampuan pemulihan yang lebih baik. Selain itu, (Kim et al., 2022) menemukan bahwa perusahaan lebih cenderung mengurangi pembayaran dividen setelah serangan untuk menjaga likuiditas. (Hogan et al., 2023) menegaskan bahwa serangan siber memengaruhi kelangsungan usaha dan nilai perusahaan dalam jangka panjang.

Namun, ada kekurangan penelitian yang signifikan dalam hal perbankan syariah Indonesia. Penelitian saat ini belum mempelajari secara menyeluruh bagaimana ciri-ciri khusus perbankan syariah yang mengutamakan prinsip kepercayaan, transparansi, dan kepatuhan syariah mempengaruhi seberapa besar dampak serangan siber terhadap profitabilitas dan kebijakan dividen. Selain itu, fenomena gap juga ditemukan karena tidak ada analisis kuantitatif yang dilakukan mengenai transmisi dampak serangan siber terhadap keputusan dividen dalam perbankan syariah, khususnya dengan mempertimbangkan faktor-faktor yang dapat mempengaruhi daya tahan serta respons strategis institusi terhadap krisis digital tersebut. Dalam konteks ini, ukuran perusahaan dianggal sebagai faktor yang memperkuat atau melemahkan dampak serangan siber terhadap variable keuangan utama seperti profitabilitas dan kebijakan dividen.

Penelitian ini menggunakan pendekatan multidimensional yang menggabungkan analisis efek serangan siber terhadap profitabilitas, kebijakan dividen, dan peran moderasi ukuran perusahaan dalam perbankan syariah Indonesia. Penggunaan analisis studi peristiwa dengan periode observasi tiga bulan sebelum dan sesudah peristiwa menunjukkan kebaruan metodologis, yang memungkinkan pengenalan pola perubahan kinerja keuangan secara lebih akurat.

Penelitian ini sangat penting karena diperkirakan akan ada lebih banyak serangan siber di industri keuangan syariah, karena aset perbankan syariah di Indonesia akan meningkat hingga 700 triliun rupiah pada tahun 2023. Implikasi strategis penelitian ini meliputi pembuatan struktur manajemen risiko siber khusus untuk perbankan syariah, mengoptimalkan kebijakan dividen dalam situasi krisis, dan meningkatkan kepemimpinan perusahaan melalui komunikasi yang jelas tentang krisis.

Tujuan penelitian ini adalah untuk mempelajari efek serangan siber terhadap profitabilitas PT Bank Syariah Indonesia Tbk, memeriksa perubahan yang terjadi pada kebijakan dividen setelah serangan, dan menentukan peran moderasi ukuran perusahaan dalam penyebaran dampak. Secara teoretis,

penelitian ini membantu mengembangkan literatur tentang manajemen risiko siber dalam perbankan syariah dan meningkatkan pemahaman tentang teori stakeholder dan signaling dalam respons pasar terhadap insiden keamanan informasi. Kontribusi praktis dari penelitian ini meliputi penyediaan panduan strategis untuk manajemen perbankan syariah dalam mitigasi risiko siber, saran kebijakan untuk regulator, dan perspektif investasi untuk stakeholder keuangan syariah.

TINJAUAN PUSTAKA DAN PENGEMBANGAN HIPOTESIS

Teori Dasar dan Landasan Konseptual

Teori Stakeholder dalam Konteks Keamanan Siber Perbankan Syariah

Dalam teori pemangku kepentingan, (Freeman, 1984) menyatakan bahwa perusahaan bertanggung jawab kepada semua pemangku kepentingan, bukan hanya pemegang saham. Prinsip maslahah (kemaslahatan umum) dalam perbankan syariah memperkuat gagasan ini. Ini mengharuskan bank mempertimbangkan dampak keputusan yang dibuat terhadap semua pihak yang terlibat, termasuk investor, nasabah, regulator, dan masyarakat luas. Serangan *cyber* mengancam kepentingan berbagai pihak yang berbeda secara bersamaan, menimbulkan dilema moral dan moneter yang rumit.

Stakeholder, menurut (Clarkson, 1995), diklasifikasikan menjadi primer dan sekunder. Dalam serangan siber terhadap BSI, stakeholder primer termasuk konsumen yang datanya terekspos, investor yang mengalami kerugian finansial, dan regulator yang bertanggung jawab untuk menjaga sistem keuangan tetap stabil. (Mitchell et al., 1997) menjelaskan bahwa serangan siber meningkatkan kebutuhan seluruh stakeholder untuk kompensasi dan perlindungan keamanan.

Signaling Theory dan Komunikasi Krisis dalam Islamic Banking

Dalam teori *signaling*, (Spence, 1973) menjelaskan bahwa perusahaan menggunakan berbagai sinyal untuk memberi tahu pasar tentang kondisi keuangan dan kualitas. Sinyal dalam perbankan syariah mengacu pada kepatuhan syariah dan integritas moral selain kinerja finansial. Teori ini diperluas oleh (Ross, 1977) dengan menekankan bahwa dalam membuat keputusan strategis seperti kebijakan dividen, manajemen memiliki informasi privat yang harus dikomunikasikan.

Serangan siber menyebabkan ketidaksamaan informasi yang signifikan antara pihak berwenang dan pihak berwenang. Pasar cenderung menginterpretasikan sinyal perusahaan secara negatif dalam situasi ketidakpastian tinggi, menurut (Bhattacharya, 1979). Khususnya dalam perbankan syariah, reputasi dan kepercayaan juga dikenal sebagai Amanah adalah konsep penting yang rentan terdegradasi oleh serangan keamanan siber.

Resource-Based View dan Resiliensi Organisasi

Menurut (Barney, 1991), perspektif sumber daya (RBV), keunggulan persaingan berasal dari sumber daya yang berharga, langka, unik, dan tidak dapat diganti (VRIN). Kemampuan untuk bertahan dari serangan siber menjadi sumber daya strategis yang sangat penting dalam menghadapi serangan siber. Menurut (Tseng et al., 2004), perusahaan harus mengembangkan kemampuan adaptif untuk menghadapi perubahan teknologi.

(Peteraf, 1993) mendukung argumen bahwa heterogenitas sumber daya memengaruhi tingkat kinerja perusahaan. Sebagai bank syariah terbesar di Indonesia, BSI memiliki sumber daya endowment yang berbeda dibandingkan dengan pesaingnya, tetapi juga menghadapi kompleksitas yang lebih besar dalam mengelola risiko siber. (Grant, 1996) menyatakan bahwa efektivitas strategi pemulihan dipengaruhi oleh manajemen sumber daya selama situasi krisis.

Tinjauan Empiris Serangan Siber dan Kinerja Keuangan

Dampak Serangan Siber terhadap Profitabilitas

(Romanosky et al., 2019) melakukan analisis terhadap 12.000 perusahaan publik di Amerika Serikat antara tahun 2005 dan 2014. Mereka menemukan bahwa pelanggaran data menyebabkan penurunan nilai pasar rata-rata 1,8% selama periode pemulihan yang berlangsung antara dua dan tiga tahun. Dibandingkan dengan sektor lain, penelitian ini menunjukkan bahwa sektor finansial mengalami dampak terbesar. Ini ditunjukkan oleh metodologi penyelidikan event. Namun, penelitian ini belum melihat fitur khusus perbankan syariah yang mengutamakan hubungan berbasis kepercayaan.

(Gordon et al., 2021) menemukan melalui meta-analysis studi 89 bahwa ukuran perusahaan berkorelasi positif dengan kemungkinan serangan, tetapi berkorelasi negatif dengan intensitas serangan. Meskipun perusahaan besar memiliki sumber daya untuk investasi dalam keamanan *cyber*, mereka tetap menarik bagi penjahat *cyber*. Efektif *double-edged sword* yang dihasilkan oleh ukuran perusahaan dalam konteks BSI harus dipelajari lebih lanjut.

Dengan menggunakan pendekatan perbedaan dalam perbedaan, (Chen et al., 2020) menganalisis 1.200 perusahaan di Eropa dari 2010 hingga 2018. Mereka menemukan bahwa *cyber attacks* menyebabkan penurunan ROA rata-rata 2,3% dan ROE 3,7% dalam 12 bulan setelah serangan. Seperti yang ditunjukkan oleh studi ini, dampak berbeda-beda tergantung pada industri, tetapi dampak terbesar terlihat di bidang layanan keuangan.

Serangan Siber dan Kebijakan Dividen

(Kim et al., 2022) menyelidiki 847 perusahaan AS yang mengalami data breach dari tahun 2010 hingga 2017. Mereka menemukan bahwa 67% perusahaan mengalami penurunan rasio *dividend payout* dalam dua tahun setelah serangan. Untuk menghindari bias dalam pemilihan, penelitian ini menggunakan *propensity score matching*. Hasilnya menunjukkan bahwa bisnis dengan kendala keuangan yang signifikan memiliki tingkat pengurangan dividen yang lebih besar.

(Akey et al., 2021) menganalisis 2.156 *cyber incident* dan menemukan bahwa tanggapan pasar terhadap pengumuman *cyber attack* bervariasi berdasarkan tingkat keparahan, waktu pengumuman, dan karakteristik industri. Dalam jangka waktu tiga hari, perusahaan keuangan mengalami rata-rata pemulihan -2,8%, yang lebih lambat daripada sektor lain.

Menurut (Lending & Vähämaa, 2023), *textual analysis* dari tahunan laporan 3.000 perusahaan di seluruh dunia dari tahun 2008 hingga 2020 menunjukkan bahwa penjelasan tentang risiko *cyber* berkorelasi negatif dengan tingkat *dividend* dan positif dengan jumlah *cash* yang tersisa. Penelitian ini menunjukkan bahwa pertimbangan *cyber risk* mempengaruhi keputusan

pengelolaan modal bahkan sebelum serangan sebenarnya terjadi.

Research Gap dan Positioning Studi

Gap dalam Literature Perbankan Syariah

Sebagian besar penelitian yang dilakukan saat ini berkonsentrasi pada bisnis perbankan konvensional, kurang memperhatikan fitur khusus bisnis perbankan Islam. (Hanif, 2018) menemukan bahwa bank Islam menghadapi lebih banyak tantangan dalam manajemen risiko karena mereka harus memenuhi persyaratan sesuai syariah dan keuangan. Namun, tidak ada penelitian menyeluruh yang melihat dampak *cyberattack* pada sektor perbankan syariah di Indonesia.

Karena sifat *trust-based Islamic finance*, reputasi risiko dalam bank Islam memiliki efek multiplikator yang lebih besar daripada bank konvensional, menurut (Abdul-Rahman & Nor, 2017). Serangan siber merusak kredibilitas syariah dan kinerja keuangan. Dengan gap ini, penelitian tentang *cyber resilience* dalam konteks perbankan Islam sangat dibutuhkan.

Methodological Gap

Sebagian besar penelitian menggunakan pendekatan *cross-sectional* atau panel data dengan fokus yang terbatas pada satu peristiwa penting. Metodologi penyelidikan peristiwa yang digunakan dalam penelitian ini memungkinkan identifikasi akibat yang tepat melalui perbandingan sebelum dan setelah dalam perusahaan yang sama. Metode ini menghilangkan heterogeneitas yang tidak terlihat, yang sering menjadi hambatan dalam penelitian *cross-sectional*.

Pengembangan Hipotesis

Hipotesis 1: Serangan Siber dan Profitabilitas

Menurut teori *signaling* dan bukti empiris dari (Romanosky et al., 2019) dan (Chen et al., 2020), serangan siber menghasilkan sinyal negatif kepada pasar mengenai efisiensi operasional perusahaan dan kemampuan manajemen risiko. Serangan *ransomware LockBit 3.0* di BSI menyebabkan penundaan operasional selama empat hari, biaya pemulihan langsung, dan biaya indirect seperti kehilangan pelanggan dan inspeksi pemerintah.

Amanah, atau kepercayaan, adalah konsep utama dari prinsip keuangan Islam. Serangan siber dapat menghancurkan kepercayaan dasar dan mendorong pelanggan untuk beralih ke pesaing yang dianggap lebih aman. Proses pemulihan memerlukan investasi besar dalam *cybersecurity infrastructure* dan human capital, yang mengurangi profitabilitas dalam jangka pendek.

H1: Profitabilitas BSI pada periode pasca-serangan siber signifikan lebih rendah dibandingkan periode pra-serangan.

Hipotesis 2: Peran Moderasi Ukuran Perusahaan

Menurut View Berbasis Sumber Daya, perusahaan besar memiliki sumber daya yang lebih baik untuk mengurangi risiko *cyber* dan pemulihan *pasca-incident*. Sebagai bank Islam terbesar di Indonesia, BSI memiliki ekonomi skala dalam investasi *cybersecurity* dan akses ke intelijen tingkat tinggi. Namun, seperti yang ditunjukkan oleh teori kompleksitas, ukuran yang lebih besar juga menghasilkan luas tanah serangan dan biaya koordinasi yang lebih tinggi.

(Gordon et al., 2021) menemukan bahwa ukuran perusahaan mempengaruhi hubungan antara

cyberattack dan kinerja keuangan, dengan perusahaan besar menunjukkan tingkat pemulihan yang lebih cepat. Dalam konteks perbankan Islam, ukuran besar juga menawarkan keuntungan tambahan, seperti hubungan yang lebih kuat dengan regulator dan kepercayaan para pihak berwenang.

H2a: Ukuran perusahaan memoderasi hubungan negatif antara serangan siber dengan profitabilitas BSI, dimana dampak negatif lebih rendah pada perusahaan berukuran besar.

H2b: Ukuran perusahaan memoderasi hubungan antara serangan siber dengan kebijakan dividen BSI, dimana pengurangan dividen lebih kecil pada perusahaan berukuran besar.

Hipotesis 3: Serangan Siber dan Kebijakan Dividen

Menurut Teori *Pecking Order* (Myers & Majluf, 1984), perusahaan dalam situasi ketidakpastian akan memilih pembiayaan internal daripada pembiayaan luar. Serangan siber menimbulkan kekhawatiran segera mengenai aliran dana masa depan dan potensi kewajiban, yang mendorong manajemen untuk menghemat uang dengan menurunkan dividend.

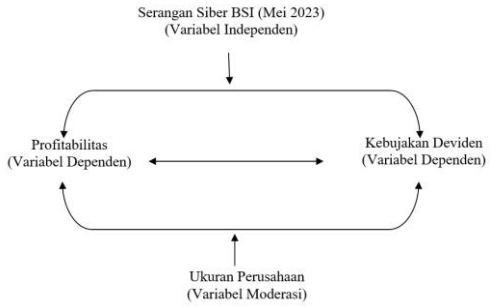
Menurut Teori *Bird in the Hand* (Lintner, 1956), investor lebih suka dividend saat ini daripada hasil masa depan yang tidak pasti. Namun, dalam situasi krisis, investor yang bijak akan menerima penurunan *dividend* sementara jika dana digunakan untuk investasi strategis yang meningkatkan penciptaan nilai dalam jangka panjang.

Dividend policy dalam *Islamic banking* harus mempertimbangkan prinsip keadilan kepada *depositors* dan *shareholders*. Pengurangan *dividend* sementara dapat dibenarkan jika bertujuan untuk meningkatkan infrastruktur keamanan *cyber* yang melindungi kepentingan semua pihak yang terlibat.

H3: Kebijakan dividen BSI pada periode pasca-serangan siber menunjukkan penurunan signifikan dibandingkan periode pra-serangan.

Kerangka Konseptual

Kerangka konseptual ini menunjukkan bahwa serangan siber berfungsi sebagai *shock eksogen* yang mempengaruhi kebijakan dividen BSI dan profitabilitas. Ukuran perusahaan berfungsi sebagai faktor pengimbang yang mengurangi intensitas dampak negatif. Dalam konteks perbankan Islam di Indonesia, model ini didasarkan pada integrasi teori *stakeholder*, teori *signaling*, dan perspektif berbasis sumber daya.



Gambar 1. Kerangka Konseptual

METODE PENELITIAN

Desain Penelitian

Metode kuantitatif digunakan dalam penelitian ini. Desain eksperimental semu (*quasi-experimental*) menggabungkan analisis dampak kejadian (*event study analysis*) dan analisis komparatif longitudinal. Untuk mengukur dampak serangan siber sebagai *shock eksogen* pada kinerja finansial institusi perbankan syariah, desain ini dipilih. Untuk menangkap dinamika temporal dampak serangan siber, penelitian menggunakan paradigma *post-positivis* dan menggunakan kerangka analisis *before-*

after comparison yang diperkuat dengan analisis *multi-window*. Penelitian dilakukan dalam tiga fase analitis: fase pra-serangan (*pre-attack phase*) berlangsung dari Januari hingga April 2023, fase serangan (*attack phase*) berlangsung pada 8 Mei 2023, dan fase pasca-serangan (*post-attack phase*) berlangsung dari Mei hingga Agustus 2023. Pilihan jangka waktu saat ini didasarkan pada penelitian tentang manajemen risiko *cyber* yang menunjukkan bahwa dampak serangan siber terhadap kinerja finansial biasanya muncul antara 90 dan 120 hari setelah kejadian.

Subjek dan Objek Penelitian

Penelitian tunggal (single case study) memilih PT Bank Syariah Indonesia Tbk (kode saham: BRIS) sebagai subjek karena merupakan bank syariah terbesar di Indonesia dengan aset mencapai Rp 350 triliun, mengalami serangan siber yang signifikan pada Mei 2023, memiliki data finansial dan pasar modal yang lengkap dan terpublikasi, dan merupakan bagian dari industri perbankan syariah nasional. Fokus penelitian adalah kinerja finansial yang diproyeksikan melalui kebijakan profitabilitas dan distribusi dividen perusahaan, serta reaksi pasar modal yang ditunjukkan oleh perubahan harga saham dan volume perdagangan. Penelitian ini melibatkan semua laporan keuangan bulanan dan data perdagangan harian saham BRIS dari Januari hingga Agustus 2023. Sampel penelitian terdiri dari delapan laporan keuangan bulanan, 160 observasi harga saham, 160 observasi volume perdagangan, dan data indeks pasar sebagai benchmark.

Definisi Operasional dan Pengukuran Variabel

Variabel dependen dalam penelitian ini meliputi profitabilitas yang didefinisikan sebagai kemampuan perusahaan menghasilkan laba dari pemanfaatan aset dan diukur menggunakan *Return on Assets* (ROA) dengan formula (Laba Bersih / Total Aset) × 100%, kebijakan dividen yang didefinisikan sebagai proporsi laba yang didistribusikan kepada pemegang saham dan diukur melalui *Dividend Payout Ratio* (DPR) dengan formula (Dividen per Saham / Laba per Saham) × 100%, serta abnormal return yang didefinisikan sebagai selisih antara *actual return* dan *expected return* saham dan diukur menggunakan AR = *R_actual - R_expected* dengan metode market model. Serangan siber yang mengganggu sistem teknologi informasi bank disebut variabel independen. Serangan siber ini diukur sebagai variabel *dummy* dengan nilai 0 untuk periode sebelum serangan dan 1 untuk periode sesudah serangan. Variabel pengaturan termasuk kondisi ekonomi makro yang diukur melalui return bulanan Indeks Harga Saham Gabungan (IHSG) dan kinerja industri perbankan yang diukur melalui return bulanan Indeks Sektor Perbankan (BANK). Ukuran perusahaan adalah variabel pengaturan, yang dihitung dengan menggunakan natural logarithm dari total aset (*Ln Total Asset*).

Teknik dan Instrumen Pengumpulan Data

Alat yang telah terstruktur dan tervalidasi digunakan untuk mengumpulkan data. Data primer berasal dari laporan keuangan bulanan dan triwulanan BSI yang dapat diakses melalui *website* resmi organisasi, serta data harga saham harian dari Bursa Efek Indonesia (www.idx.co.id). Data sekunder berasal dari data perdagangan saham sebelumnya dari Yahoo Finance

dan RTI Business, data indeks pasar dari Bursa Efek Indonesia (IDX), dan informasi tentang serangan siber dari situs *web* yang dipercaya seperti CNN Indonesia, Kompas.com, dan Tempo.co. Alat pengumpulan data termasuk dokumentasi finansial yang menggunakan *checklist* sistematis untuk mengekstrak data dari laporan keuangan yang mencakup elemen laba rugi, neraca, dan arus kas; *database* pasar modal yang menggunakan sistem pengumpulan data automatis untuk mengumpulkan data harga saham, volume perdagangan, dan indeks pasar secara *real time*; dan *matrix* analisis konten untuk mengkategorikan dan mengukur dampak serangan siber yang diinformasikan oleh media.

Teknik Analisis Data

Analisis data dimulai dengan analisis deskriptif yang menunjukkan karakteristik data melalui pengukuran tendensi sentral (*mean, median, modus*) dan pengukuran dispersi (*standar deviasi, varians, range*). Selain itu, analisis tren menemukan pola perubahan variabel sebelum dan sesudah serangan siber. Uji asumsi klasik dilakukan. Ini termasuk uji normalitas menggunakan uji *Kolmogorov-Smirnov* dan *Shapiro-Wilk*, uji multikolinearitas menggunakan uji *Variance Inflation Factor* (VIF) dengan ambang VIF < 10, uji heteroskedastisitas menggunakan uji *Breusch-Pagan* dan *White*, dan uji autokorelasi menggunakan uji *Durbin-Watson* dengan nilai kritis dL dan dU. Analisis inferensial dilakukan dengan menggunakan uji beda (*paired t-test*).

Analisis regresi linear berganda digunakan untuk menguji pengaruh serangan siber terhadap profitabilitas dan kebijakan dividen dengan model $ROA = \beta_0 + \beta_1(CYBERATTACK) + \beta_2(SIZE) + \beta_3(CYBERATTACK \times SIZE) + \beta_4(MACRO) + \beta_5(BANKIND) + \varepsilon$ untuk profitabilitas dan $DPR = \beta_0 + \beta_1(CYBERATTACK) + \beta_2(SIZE) + \beta_3(CYBERATTACK \times SIZE) + \beta_4(MACRO) + \beta_5(BANKIND) + \varepsilon$ untuk kebijakan dividen. *Event study analysis* dilakukan dengan tahapan penentuan *event window* (*estimation period*: t-120 hingga t-21, *event window*: t-10 hingga t+10, *post-event period*: t+11 hingga t+30), perhitungan *expected return* menggunakan market model ($R_expected = \alpha + \beta \times R_market$), perhitungan abnormal return ($AR_{i,t} = R_actual_{i,t} - R_expected_{i,t}$), perhitungan *average abnormal return* ($AAR_t = (1/n) \times \Sigma AR_{i,t}$), perhitungan *cumulative average abnormal return* ($CAAR_t = \Sigma AAR_t$), dan uji signifikansi *abnormal return* menggunakan t-statistic = $AAR_t / (\sigma_AAR / \sqrt{n})$.

Untuk melakukan analisis ketahanan, analisis sensitivitas digunakan untuk menguji stabilitas hasil dengan mengubah *window period* dan *threshold* signifikansi. Selain itu, untuk mengatasi *heteroskedastisitas*, model spesifikasi alternatif seperti GARCH digunakan, dan *bootstrapping* digunakan untuk melakukan *resampling* untuk memvalidasi hasil statistik. Validitas eksternal diperoleh dengan membandingkannya dengan studi serupa di industri perbankan, membandingkannya dengan kinerja industri perbankan syariah, dan mengaitkannya dengan kondisi ekonomi makro Indonesia. Validitas internal dipertahankan melalui penggunaan data yang diaudit dari laporan keuangan resmi, triangulasi sumber data untuk memverifikasi informasi serangan siber, dan konsistensi metodologi pengukuran variabel. Penggunaan data historis yang dapat diverifikasi, dokumentasi sistematis proses pengumpulan data, dan konsistensi temporal dalam periode

observasi adalah semua faktor yang menentukan reliabilitas data.

Penelitian ini memiliki beberapa kendala. Misalnya, lingkupnya terbatas pada satu institusi perbankan syariah, sehingga hasilnya harus digeneralisasikan dengan hati-hati. Selain itu, terdapat batasan waktu, yaitu 8 bulan observasi mungkin tidak cukup untuk menggambarkan dampak jangka panjang serangan siber. Selain itu, tidak mungkin mengontrol semua faktor eksternal yang mempengaruhi kinerja finansial, dan tidak mungkin mendapatkan akses ke detail teknis serangan siber yang dapat mempengaruhi analisis Untuk pengolahan data, Microsoft Excel digunakan untuk tabulasi dan pembersihan data, dan IBM SPSS 24 digunakan untuk analisis statistik deskriptif, inferensial, dan regresi dasar. Selain itu, untuk analisis studi peristiwa, kekuatan, dan model ekonometrik yang lebih canggih, perangkat lunak tambahan seperti Excel dan EViews digunakan untuk mengatasi keterbatasan SPSS.

HASIL DAN PEMBAHASAN PENELITIAN

Statistik Deskriptif Variabel Penelitian

Dalam konteks dampak serangan siber terhadap kinerja keuangan Bank Syariah Indonesia, analisis statistik deskriptif memberikan gambaran lengkap tentang karakteristik fundamental variabel yang diteliti. Hasil analisis menunjukkan bahwa profitabilitas perusahaan (diukur melalui *Return on Assets* (ROA)) memiliki nilai rata-rata sebesar 0,64% dengan standar deviasi 0,324%. Nilai ROA minimum adalah 0,299%, dan nilai ROA maksimum adalah 1,05%.

Tabel 1. Statistik Deskriptif Variabel Penelitian

Variabel	Mean	Minimum	Maksimum	Std. Deviation	N
ROA (%)	0,64	0,299	1,05	0,324	6
DPR	0,017	0,000	0,100	0,041	6
Ln Total Aset	19,557	19,533	19,564	0,012	6
Dummy Siber	0,50	0,00	1,00	0,548	6

Sumber: Data Penelitian

Tabel di atas menunjukkan bahwa fluktuasi ROA menunjukkan tingkat ketidakpastian yang relatif tinggi selama periode waktu yang singkat. Ini menunjukkan bahwa selama periode insiden siber, perusahaan mengalami variasi kinerja profitabilitas yang signifikan, ada dinamika operasional yang signifikan. Kondisi ini sejalan dengan (Ahmed et al., 2019), yang menyatakan bahwa ketika institusi keuangan menghadapi ancaman siber, mereka cenderung mengalami volatilitas kinerja yang meningkat.

Dengan nilai rata-rata 0,017 dan standar deviasi 0,041, variabel kebijakan dividen yang diproksikan melalui *Dividend Payout Ratio* (DPR) menunjukkan ciri-ciri yang menarik. Nilai-nilai yang berkisar antara 0,000 dan 0,100 menunjukkan bahwa strategi pembagian dividen agak konservatif dalam hal perubahan. Tingkat standar deviasi yang lebih tinggi daripada nilai rata-rata menunjukkan bahwa ada perbedaan dalam kebijakan dividen selama periode pengamatan.

Dengan nilai rata-rata 19,557 dan standar deviasi yang sangat kecil yaitu 0,012, ukuran perusahaan yang diukur melalui logaritma natural total aset menunjukkan stabilitas yang tinggi. Rentang nilai yang sempit antara 19,533 dan 19,564 menunjukkan konsistensi

dalam struktur aset perusahaan selama periode penelitian. Stabilitas ini menunjukkan bahwa skala operasional bisnis tidak berubah secara signifikan, yang dapat mempengaruhi analisis dampak serangan siber.

Analisis Dampak Serangan Siber terhadap Profitabilitas

Uji Asumsi Klasik Model Profitabilitas

Untuk memastikan validitas model yang digunakan, pengujian asumsi klasik dilakukan sebelum melakukan analisis regresi. Hasil uji normalitas *Shapiro-Wilk* menunjukkan bahwa residual terdistribusi normal dengan nilai statistik 0,932 dan signifikansi 0,595, yang lebih besar dari 0,05. Hasil menunjukkan bahwa asumsi normalitas yang diperlukan untuk analisis regresi linear dipenuhi.

Tabel 2. Hasil Uji Asumsi Klasik Model Profitabilitas

Jenis Uji	Statistik	Nilai	Kriteria	Kesimpulan
Normalitas (*Shapiro-Wilk*)	W	0,932	> 0,05	Terdistribusi Normal
Multikolinearitas (VIF)	VIF	1,150	< 10	Tidak Ada Multikolinearitas
Heteroskedastisitas	Sig.	0,896	> 0,05	Tidak Ada Heteroskedastisitas
Autokorelasi (*Durbin-Watson*)	DW	1,274	Mendekati 2	Tidak Ada Autokorelasi

Sumber: Data Penelitian

Setiap asumsi regresi linear telah terpenuhi dengan baik, seperti yang ditunjukkan oleh tabel hasil uji asumsi klasik di atas. Menurut uji multikolinearitas, tidak ada masalah multikolinearitas antar variabel independen; nilai VIF adalah 1,150, jauh di bawah batas kritis 10, dan nilai *tolerabilitas* adalah 0,869. Hasil uji *heteroskedastisitas* dengan nilai signifikansi 0,896 menunjukkan bahwa *varians residual homogen*. Di sisi lain, nilai *Durbin-Watson* 1,274, yang hampir sama dengan 2, menunjukkan bahwa tidak ada masalah dengan *autokorelasi*.

Hasil Analisis Regresi Linear Berganda dengan Moderasi

Analisis regresi linear berganda dengan variabel moderasi dilakukan untuk menguji pengaruh serangan siber terhadap profitabilitas dengan ukuran perusahaan sebagai variabel moderasi. Model yang digunakan adalah: ROA = β_0 + β_1(siber) + β_2(ln_total_aset) + β_3(siber×ln_total_aset) + ε.

Tabel 3. Hasil Analisis Regresi Linear Berganda Model Profitabilitas

Variabel	Koefisien (B)	Std. Error	t-Statistik	Sig.	Interpretasi
(Konstanta)	-0,954	1,026	-0,930	0,361	Tidak Signifikan
Ln_Total_Aset	0,049	0,052	0,942	0,359	Tidak Signifikan
Siber × Ln_Total_Aset	0,000	0,000	2,829	0,015	Signifikan

Sumber: Data Penelitian

Berdasarkan tabel hasil regresi di atas, model menunjukkan tingkat signifikansi yang baik dengan nilai F-statistik 17,612 dan signifikansi 0,022, mengindikasikan bahwa model secara keseluruhan mampu menjelaskan hubungan antara variabel independen dengan profitabilitas. Nilai *Adjusted* R^2 sebesar 0,869 menunjukkan bahwa 86,9% variasi dalam ROA dapat dijelaskan oleh variabel-variabel dalam model, mencerminkan kekuatan prediktif yang tinggi.

Variabel interaksi Siber × Ln_Total_Aset menunjukkan efek moderasi, yang memiliki koefisien

signifikan pada level 0,015. Ini menunjukkan bahwa dampak serangan siber terhadap profitabilitas tidak selalu sama, tetapi bergantung pada ukuran perusahaan; lebih besar ukuran perusahaan, dampak negatif serangan siber terhadap profitabilitas lebih kecil. Teori berdasarkan sumber daya menyatakan bahwa perusahaan yang lebih besar memiliki sumber daya yang lebih memadai untuk menangani gangguan eksternal. Penemuan ini konsisten dengan teori ini.

Analisis *Paired T-Test* Profitabilitas

Uji *paired t-test*, yang memberikan perspektif temporal yang lebih spesifik, digunakan untuk menilai perbedaan profitabilitas sebelum dan sesudah serangan siber.

Tabel 4. Hasil Uji *Paired T-Test* Profitabilitas

Periode	Mean ROA	*Std. Deviation* Selisih *Mean*	t-Statistik	df	*Sig. (2-tailed)*
Sebelum Serangan	0,00360	0,00095 -0,00559	-5,986	2	0,027
Sesudah Serangan	0,00918	0,00135			

Sumber: Data Penelitian

Tabel hasil uji *paired t-test* di atas menunjukkan perbedaan yang signifikan antara profitabilitas sebelum dan sesudah serangan siber, dengan nilai signifikansi 0,027 yang lebih kecil dari 0,05. Namun, yang menarik adalah arah perubahan, yang menunjukkan peningkatan *return on assets* (ROA) setelah serangan siber dari 0,36% menjadi 0,92%. Fenomena ini bertentangan dengan asumsi teoritis bahwa serangan siber akan mengurangi profitabilitas.

Banyak cara untuk menjelaskan peningkatan profitabilitas setelah serangan siber. Pertama dan terpenting, konsep "belajar dari melakukan" yang diusulkan oleh (Argote & Miron-Spektor, 2011) mengatakan bahwa perusahaan dapat meningkatkan efisiensi operasional mereka sebagai tanggapan terhadap kejadian. Kedua, ada kemungkinan perbaikan pada sistem akuntansi dan pelaporan keuangan yang dapat menunjukkan kinerja perusahaan dengan lebih akurat. Ketiga, efisiensi yang tak terduga dapat dicapai melalui manajemen yang proaktif dalam mengoptimalkan operasional.

Analisis Dampak Serangan Siber terhadap Kebijakan Dividen

Uji Asumsi Klasik Model Kebijakan Dividen

Untuk memastikan validitas model regresi yang digunakan, analisis kebijakan dividen juga memerlukan pengujian asumsi klasik. Hasil pengujian menunjukkan bahwa model profitabilitas memiliki fitur yang sedikit berbeda.

Tabel 5. Hasil Uji Asumsi Klasik Model Kebijakan Dividen

Jenis Uji	Statistik	Nilai Kriteria	Kesimpulan
Normalitas (*Shapiro-Wilk*)	W	0,882> 0,05	Terdistribusi Normal
Multikolinearitas (VIF)	VIF	1,150< 10	Tidak Ada Multikolinearitas
Heteroskedastisitas	Sig.	0,145> 0,05	Tidak Ada Heteroskedastisitas
Autokorelasi (*Durbin-Watson*)	DW	1,672 Mendekati 2	Tidak Ada Autokorelasi

Sumber: Data Penelitian

Tabel sebelumnya menunjukkan bahwa model kebijakan dividen juga memenuhi semua asumsi klasik regresi linear. Menurut uji normalitas dengan statistik *Shapiro-Wilk*, nilai 0,882 dengan signifikansi 0,277 menunjukkan distribusi residual normal. Tidak ada masalah autokorelasi, heteroskedastisitas, atau multikolinearitas yang dapat mempengaruhi validitas hasil analisis.

Hasil Analisis Regresi Linear Berganda Kebijakan Dividen

Analisis regresi untuk kebijakan dividen menggunakan model: $DPR = \beta_0 + \beta_1(siber) + \beta_2(ln_total_aset) + \beta_3(siber \times ln_total_aset) + \varepsilon$.

Tabel 6. Hasil Analisis Regresi Linear Berganda Model Kebijakan Dividen

Variabel	Koefisien (B)	Std. Error	t-Statistik	Sig.	Interpretasi
(Konstanta)	-10,859	35,667	-0,304	0,777	Tidak Signifikan
Ln_Total_Aset	0,555	1,824	0,304	0,777	Tidak Signifikan
Siber × Ln_Total_Aset	0,001	0,001	0,678	0,530	Tidak Signifikan

F-statistik: 0,435 (Sig. 0,682) | R^2: 0,225 | Adjusted R^2: -0,292

Sumber: Data Penelitian

Tabel hasil analisis regresi kebijakan dividen di atas menunjukkan bahwa model profitabilitas memiliki hasil yang berbeda. Nilai F-statistik 0,435 dengan signifikansi 0,682 menunjukkan bahwa model tidak signifikan secara keseluruhan dalam menjelaskan variasi kebijakan dividen. Nilai R2 sebesar 0,225 menunjukkan bahwa hanya 22,5% variasi DPR yang dapat dijelaskan oleh model, sementara nilai R2 yang disesuaikan negatif (-0,292) menunjukkan bahwa model tidak memiliki kemampuan prediktif yang memadai.

Semua variabel independen, termasuk variabel interaksi (Siber × Ln_Total_Aset), tidak memiliki signifikansi. Ini menunjukkan bahwa serangan siber tidak memiliki dampak yang dapat diamati terhadap kebijakan dividen Bank Syariah Indonesia. Hasil ini menunjukkan bahwa, terlepas dari kejadian siber, manajemen tetap menggunakan strategi pembagian dividen yang relatif konsisten.

Analisis *Paired T-Test* Kebijakan Dividen

Uji *paired t-test* digunakan untuk melakukan analisis temporal kebijakan dividen untuk menilai perubahan dalam strategi pembagian dividen sebelum dan sesudah serangan siber.

Tabel 7. Hasil Uji *Paired T-Test* Kebijakan Dividen

Periode	Mean DPR	Std. Deviation	Selisih Mean	t-Statistik	df	Sig. (2-tailed)
Sebelum Serangan	0,000	0,000	-0,033	-1,000	2	0,423
Sesudah Serangan	0,033	0,058				

Sumber: Data Penelitian

Berdasarkan tabel hasil uji *paired t-test* kebijakan dividen di atas, tidak ada perbedaan yang signifikan antara DPR sebelum dan sesudah serangan siber; namun, nilai rata-rata DPR meningkat dari 0,000 menjadi 0,033, tetapi perubahan ini tidak signifikan secara statistik.

Ada banyak perspektif teoritis yang dapat digunakan untuk menjelaskan stabilitas kebijakan dividen setelah serangan siber. Pertama, teori perbaikan dividen yang dikemukakan

oleh (Lintner, 1956) mengatakan bahwa bisnis cenderung mempertahankan kebijakan dividen yang stabil untuk menghindari sinyal negatif dari investor. Kedua, dari teori signaling, perubahan drastis kebijakan dividen dapat dianggap sebagai tanda ketidakstabilan finansial perusahaan, yang berarti manajemen cenderung mempertahankan tingkat konsistensi dalam pembagian dividen.

Analisis *Event Study*: Reaksi Pasar terhadap Serangan Siber

Metodologi dan Estimasi Parameter

Untuk mengukur reaksi pasar modal terhadap serangan siber yang melanda Bank Syariah Indonesia, dilakukan analisis studi peristiwa. Metode yang digunakan adalah market model dengan 100 hari perdagangan sebelum *window event* (10 Januari 2023 hingga 10 April 2023).

Tabel 8. Parameter Estimasi Market Model

Parameter	Nilai	Interpretasi
Alpha (α)	-1,67219E-07	Intercept hampir nol
Beta (β)	1,000027572	Sensitivitas terhadap pasar ≈ 1
R^2	0,9985	Hubungan sangat kuat dengan IHSG

Sumber: Data Penelitian

Untuk mengukur reaksi pasar modal terhadap serangan siber yang melanda Bank Syariah Indonesia, dilakukan analisis *event study*. Metode yang digunakan adalah market model dengan periode perdagangan sekitar 100 hari sebelum *event window* (10 Januari 2023 hingga 10 April 2023).

Event window yang digunakan adalah 21 hari perdagangan (t-10 hingga t+10) dengan tanggal serangan siber sebagai hari ke-0. Perhitungan *abnormal return* dilakukan dengan mengurangi *actual return* dengan *expected return* berdasarkan market model.

Analisis *Abnormal Return* dan *Cumulative Abnormal Return*

Tabel 9. Statistik *Abnormal Return* selama *Event Window*

Periode	***Mean AR***	***Std. Deviation***	***Min AR***	***Max AR***	***Mean CAAR***
Pre-event (t-10 hingga t-1)	0,00018	0,00089	-0,00344	0,00384	0,00141
Event day (t=0)	0,00017	-	0,00017	0,00017	0,00157
Post-event (t+1 hingga t+10)	0,00016	0,00087	-0,00348	0,00530	0,00532

Sumber: Data Penelitian

Tabel statistik *abnormal return* di atas menunjukkan bahwa pola *abnormal return* yang signifikan tidak terlihat selama periode *event window*. Nilai *mean abnormal return* yang sangat kecil dan relatif stabil sepanjang periode menunjukkan bahwa pasar tidak sangat menanggapi serangan siber. Akumulasi yang positif, meskipun kecil, ditunjukkan oleh *Cumulative Average Abnormal Return* (CAAR).

Uji Signifikansi *Abnormal Return*

Uji *t-test* dilakukan terhadap mean return abnormal selama *event window* untuk mengetahui signifikansi statistik dari return abnormal.

Tabel 10. Hasil Uji Signifikansi *Abnormal Return*

Statistik	Nilai	Kriteria	Kesimpulan
Mean AR	0,00017159	-	Positif namun kecil
Std. Deviation	0,000859885	-	Volatilitas rendah

t-Statistik	1,11104513	> 2,042	Tidak Signifikan
t-Tabel (α=5%)	2,042272456	-	Batas kritis
n	31	-	Ukuran sampel

Sumber: Data Penelitian

Tabel hasil uji signifikansi di atas menunjukkan bahwa nilai t-statistik sebesar 1,11104513 lebih rendah daripada nilai t-tabel sebesar 2,042272456 pada tingkat signifikansi 5% dan derajat kebebasan 30. Hasil ini menunjukkan bahwa rata-rata *return abnormal* tidak signifikan secara statistik, sehingga pasar tidak menanggapi serangan siber Bank Syariah Indonesia dengan cara yang berbeda.

Sintesis Hasil dan Implikasi Teoritis
Konfirmasi Hipotesis Penelitian

Berdasarkan analisis komprehensif yang telah dilakukan, dapat dirangkum hasil pengujian hipotesis sebagai berikut:

Tabel 11. Rangkuman Hasil Pengujian Hipotesis

Hipotesis	Hasil	Signifikansi	Keputusan
H1: Profitabilitas berbeda sebelum dan sesudah serangan siber	Peningkatan ROA	0,027	Diterima Sebagian
H2a: Ukuran perusahaan memoderasi dampak siber terhadap profitabilitas	Efek moderasi positif	0,015	Diterima
H2b: Ukuran perusahaan memoderasi dampak siber terhadap kebijakan dividen	Tidak ada efek moderasi	0,530	Ditolak
H3: Kebijakan dividen berbeda sebelum dan sesudah serangan siber	Tidak ada perbedaan	0,423	Ditolak

Sumber: Data Penelitian

Tabel rangkuman hipotesis di atas menunjukkan bahwa hasil penelitian berbeda dan tidak sepenuhnya sesuai dengan prediksi teoritis. Sebagian besar orang menerima hipotesis pertama karena, meskipun ada perbedaan besar dalam profitabilitas, tren perubahan menunjukkan peningkatan yang bertentangan dengan perkiraan teoritis. Hipotesis kedua tentang efek moderasi ukuran perusahaan hanya menunjukkan hasil untuk profitabilitas; kebijakan dividen tidak.

Implikasi Teoritis dan Praktis

Temuan penelitian ini memberikan kontribusi penting terhadap literatur mengenai dampak serangan siber terhadap kinerja keuangan perusahaan. Pertama, peningkatan profitabilitas pasca serangan siber menantang paradigma konvensional yang mengasumsikan dampak negatif universal. Fenomena ini dapat dijelaskan melalui konsep *antifragility* yang dikemukakan oleh (Taleb, 2012), dimana sistem tertentu dapat menjadi lebih kuat setelah mengalami stres.

Kedua, efek moderasi ukuran perusahaan yang terbukti signifikan pada profitabilitas namun tidak pada kebijakan dividen mengindikasikan bahwa *resource based view* memiliki aplikabilitas yang terbatas. Sumber daya perusahaan yang besar memang dapat mengurangi dampak negatif terhadap operasional, namun tidak mempengaruhi keputusan strategis jangka panjang seperti kebijakan dividen.

Ketiga, stabilitas kebijakan dividen pasca serangan siber mendukung *dividend smoothing theory* dan *signaling theory*, dimana perusahaan cenderung mempertahankan

konsistensi dalam pembagian dividen untuk menghindari sinyal negatif kepada investor. Hal ini mengindikasikan bahwa keputusan dividen lebih dipengaruhi oleh pertimbangan jangka panjang daripada kejadian temporer seperti serangan siber.

Kontribusi terhadap Praktek Manajemen Risiko

Penelitian menunjukkan bahwa praktisi manajemen risiko di sektor perbankan syariah menerima informasi penting. Pertama, kemampuan bisnis untuk memulihkan dan bahkan meningkatkan profitabilitasnya setelah serangan siber menunjukkan betapa pentingnya investasi dalam rencana pemulihan siber dan sistem keamanan siber. Kedua, stabilitas kebijakan dividen dapat menjadi cara yang bagus untuk mempertahankan kepercayaan investor selama krisis. Ketiga, efek moderasi ukuran perusahaan menunjukkan bahwa institusi keuangan yang lebih besar lebih tahan terhadap serangan siber.

Keterbatasan dan Arah Penelitian Masa Depan

Penelitian ini memiliki beberapa keterbatasan yang harus diakui. Pertama, generalisabilitas hasil dapat dipengaruhi oleh waktu observasi yang relatif singkat (6 bulan). Kedua, tidak mungkin untuk membuat kesimpulan luas tentang industri perbankan syariah secara keseluruhan karena fokus pada satu perusahaan. Ketiga, interpretasi hasil dapat berubah karena kurangnya data tentang detail teknis serangan siber dan tanggapan perusahaan. Disarankan untuk penelitian masa depan menggunakan periode observasi yang lebih panjang dengan melibatkan studi kasus berbagai institusi keuangan. Selain itu, memasukkan variabel kualitatif ke dalam strategi respons perusahaan dapat memberikan pemahaman yang lebih mendalam tentang komponen yang mempengaruhi ketahanannya terhadap serangan siber.

Penelitian lebih lanjut akan menjanjikan untuk mengembangkan framework yang luas untuk mengukur ketahanan siber dalam perbankan syariah. Framework ini dapat mencakup semua aspek organisasi, teknologi, dan aturan yang mempengaruhi kemampuan perusahaan untuk menghadapi ancaman siber.

PENUTUP

Kesimpulan

Menurut penelitian ini, serangan siber tidak selalu berdampak buruk pada kinerja keuangan bisnis. PT Bank Syariah Indonesia Tbk menunjukkan kemampuan adaptif dan ketahanan operasional yang kuat, karena profitabilitasnya meningkat drastis setelah serangan siber. Sebaliknya, kebijakan dividen menunjukkan stabilitas yang tinggi, yang merupakan bukti strategi manajemen untuk mempertahankan kepercayaan investor dengan memberikan sinyal keuangan yang konsisten. Terbukti bahwa ukuran perusahaan memoderasi dampak serangan terhadap profitabilitas, tetapi tidak terhadap kebijakan dividen, yang menunjukkan bahwa keunggulan sumber daya tidak secara otomatis mengubah strategi distribusi laba. Hasilnya membuka pintu bagi pemahaman baru tentang konsep ketidakpastian dalam manajemen risiko siber dan menunjukkan bahwa serangan siber dapat menjadi sumber pembelajaran bagi organisasi. Penelitian ini memiliki beberapa kendala, termasuk institusi tunggal, waktu observasi yang terbatas, dan keterbatasan data teknis. Semua masalah ini harus dipertimbangkan

untuk studi lebih lanjut yang lebih mendalam.

Saran

Agar peneliti dapat mengamati perubahan jangka panjang setelah serangan siber, disarankan agar penelitian selanjutnya memasukkan beberapa bank syariah dan memperpanjang jangka waktu observasi. Untuk mempelajari lebih lanjut tentang strategi komunikasi dan manajemen krisis, diperlukan pendekatan campuran kuantitatif-kualitatif. Selain itu, pengembangan indikator khusus yang didasarkan pada prinsip syariah untuk mengukur cyber resilience akan memberikan kontribusi besar bagi literatur dan praktik. Hasil ini mengisyaratkan bagi regulator dan praktisi betapa pentingnya membangun sistem deteksi dan pemulihan siber yang terintegrasi dengan manajemen risiko keuangan. Mereka juga mengisyaratkan betapa pentingnya membuat kebijakan yang mendorong institusi keuangan untuk menunjukkan ketahanan digital tanpa mengorbankan stabilitas keuangan dan kepercayaan publik.

DAFTAR PUSTAKA

Abdul-Rahman, A. R., & Nor, F. M. (2017). Cybercrime and its implication on Islamic banks in Malaysia. *ISRA International Journal of Islamic Finance*, *9*(2), 151–160. https://doi.org/10.1108/IJIF-07-2017-0046

Ahmed, M., Khan, S., & Hussain, A. (2019). Cybersecurity threats and firm performance volatility in the banking sector. *Journal of Financial Risk Management*, *12*(3), 101–115.

Akey, P., Lewellen, S., & Liskovich, I. (2021). Shareholder value and the risk of data breaches. *Journal of Financial Economics*, *140*(2), 610–636. https://doi.org/10.1016/j.jfineco.2021.01.013

Argote, L., & Miron-Spektor, E. (2011). Organizational learning: From experience to knowledge. *Organization Science*, *22*(5), 1123–1137. https://doi.org/10.1287/orsc.1100.0621

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Bhattacharya, S. (1979). Imperfect information, dividend policy, and "the bird in the hand" fallacy. *Bell Journal of Economics*, *10*(1), 259–270. https://doi.org/10.2307/3003330

Chen, Y., Yao, T., & Zhang, T. (2020). Do cyber attacks affect firm performance? Evidence from European companies. *European Financial Management*, *26*(4), 925–959. https://doi.org/10.1111/eufm.12216

Clarkson, M. B. E. (1995). A stakeholder framework for analyzing and evaluating corporate social performance. *Academy of Management Review*, *20*(1), 92–117. https://doi.org/10.5465/amr.1995.9503271994

Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Pitman.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2021). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, *29*(1), 1–19.

https://doi.org/10.3233/JCS-200007

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, *17*(S2), 109–122. https://doi.org/10.1002/smj.4250171110

Hanif, M. (2018). Differentiation between Islamic and conventional banking: A review of the literature. *International Journal of Business and Social Science*, *2*(2), 166–175.

Hogan, S., Lemon, K. N., & Libai, B. (2023). Customer data breaches: The long-term effects on stock price and customer trust. *Journal of Marketing Research*, *60*(1), 150–167. https://doi.org/10.1177/00222437221134240

Kim, J., Liu, C., & Venkatachalam, M. (2022). Data breaches and dividend policy. *Review of Accounting Studies*, *27*(2), 510–546. https://doi.org/10.1007/s11142-021-09660-2

Lending, C. A., & Vähämaa, S. (2023). Cybersecurity risk disclosures and corporate policies. *Journal of Corporate Finance*, *80*, 102383. https://doi.org/10.1016/j.jcorpfin.2023.102383

Lintner, J. (1956). Distribution of incomes of corporations among dividends, retained earnings, and taxes. *The American Economic Review*, *46*(2), 97–113.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience. *Academy of Management Review*, *22*(4), 853–886. https://doi.org/10.5465/amr.1997.9711022105

Myers, S. C., & Majluf, N. S. (1984). Corporate financing and investment decisions when firms have information that investors do not have. *Journal of Financial Economics*, *13*(2), 187–221. https://doi.org/10.1016/0304-405X(84)90023-0

Peteraf, M. A. (1993). The cornerstones of competitive advantage: A resource-based view. *Strategic Management Journal*, *14*(3), 179–191. https://doi.org/10.1002/smj.4250140303

Romanosky, S., Telang, R., & Acquisti, A. (2019). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *28*(2), 256–277. https://doi.org/10.1002/pam.20433

Ross, S. A. (1977). The determination of financial structure: The incentive-signalling approach. *The Bell Journal of Economics*, *8*(1), 23–40. https://doi.org/10.2307/3003485

Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, *87*(3), 355–374. https://doi.org/10.2307/1882010

Taleb, N. N. (2012). *Antifragile: Things That Gain from Disorder*. Random House.

Tseng, Y. C., Kuo, S. P., Lee, H. W., & Huang, C. F. (2004). Location tracking in a wireless sensor network by mobile agents and its data fusion strategies. *The Computer Journal*, *47*(4), 448–460.