BAB I

PENDAHULUAN

A. Konteks Penelitian

Sektor perbankan merupakan bidang yang tidak lepas dari pengaruh digitalisasi, salah satunya ialah pada perbankan syariah. Hal ini dapat diketahui karena adanya disrupsi dari nasabah baru dan persaingan antar bank yang tidak lepas dari adanya digitalisasi.[1] Perbankan syariah mulai meningkatkan layanannya sehingga nasabah dapat secara mandiri memperoleh berbagai layanan atau disebut sebagai *self-service* untuk berbagai jenis transaksi dan layanan.[2] Hal ini dapat diartikan sebagai dampak dari adanya perkembangan teknologi dan informasi yang turut mempengaruhi persaingan pada sektor perbankan syariah.

Tuntutan digitalisasi perbankan diperkuat oleh berbagai faktor yang mendorong penggunaan alat digital di Indonesia, karena Indonesia merupakan negara perekonomian yang memiliki potensi besar dalam menyerap arus digitalisasi. Faktor- faktor tersebut tercermin dalam tiga aspek utama yaitu kapabilitas digital, perilaku digital, dan transaksi digital. Peluang digital mencakup potensi demografi, potensi ekonomi dan keuangan digital, serta potensi penetrasi internet sekaligus potensi

[1] M. Moeljadi, Supriati, dan Soegiri. "Generic Sharia Governance and Expertice in Indonesian Digital Islamic Bank Ecosystem." *International Journal Of Emerging Issues in IslamIc Studies,* 2 (1), 2022, 18-30.
[2] Sakti, M. A. J., Achsani, N., dan Syarifuddin, F. "Online Banking Implementation: Risk Mapping Using (ERM) Approach"*, Buletin Ekonomi Moneter dan Perbankan*, 2018, 20.

pertumbuhan konsumen. Perilaku digital mencakup keterlibatan karyawan dan penggunaan aplikasi seluler. Transaksi digital meliputi transaksi bisnis online *(e-commerce),* transaksi perbankan digital, dan transaksi uang elektronik.

Pemanfaatan alat digital pada sektor perbankan selain menawarkan kemudahan juga terdapat kekurangan seperti ancaman peretasan data. serta tantangan yang perlu dihadapi. Tantangan tersebut mencakup beberapa hal diantaranya data pribadi, risiko kebocoran data, dan risiko investasi, risiko penyalahgunaan teknologi kecerdasan buatan (AI), risiko serangan siber, risiko *outsourcing* hingga rendahnya tingkat perlindungan data.[3] Maka dalam hal ini perlunya dukungan kesiapan dari pihak Bank Syariah Indonesia dalam menghadapi tantangan dan ancaman dari serangan siber.

Dilansir dari laman KOMPAS TV pada tanggal 23 Mei 2023, terdapat kasus terkait keamanan siber yakni gangguan layanan baik *online banking* dan ATM sampai layanan *offline* di Bank Syariah Indonesia (Persero) Tbk yang terjadi selama beberapa hari. Dampak dari adanya gangguan layanan tersebut mengakibatkan nasabah mengalami kendala pada saat melakukan transaksi. Gangguan yang terjadi pada Bank Syariah Indonesia adalah akibat dari peretasan yang dilakukan oleh kelompok LockBit 3.0 melalui *ransomware* sejenis program jahat atau *malware* yang mengancam korban dengan menghancurkan serta memblokir akses ke data

[3] OJK. "Transformasi Digital Perbankan: Wujudkan Bank Digital". Artikel: Kamis, 13 Oktober 2022. https://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/40774 diakses pada tanggal 26 Mei 2023.

juga sistem penting hingga meminta tebusan uang sebagai jaminan atas data yang diretas. Kelompok LockBit 3.0 mengklaim telah berhasil mencuri 1,5 Terabyte data pribadi dari server Bank Syariah Indonesia dan meminta tebusan sebesar 20 juta dollar AS atau Rp 295 miliar.[4]

Untuk menghadapi adanya gangguan layanan yang disebabkan oleh kelompok LockBit 3.0, maka diperlukan manajemen risiko *(risk management)* yang efektif sebagai langkah untuk menghadapi adanya serangan siber. Hal ini karena, manajemen risiko dilakukan secara berkelanjutan sebagai sarana untuk menginformasikan potensi kerugian yang mungkin saja bisa terjadi, sehingga dapat membantu pengelola bank dalam membuat keputusan yang tepat. Bagi Bank Indonesia selaku pengawas Bank, penerapan manajemen risiko akan memudahkan dalam menganalisis peluang kerugian suatu Bank, yang pada prosesnya bisa berdampak buruk pada sektor perbankan.[5] Dengan demikian, Bank Syariah Indonesia akan dapat menjaga reputasi dan citranya sebagai institusi yang aman dan terpercaya bagi nasabahnya.

---

[4] Johannes Mangihot. "Kasus BSI Bukti Keamanan Siber di Indonesia Lemah, dari Skala Satu sampai 10 Skornya 3". *(KOMPAS TV).* https://www.kompas.tv/nasional/409259/kasus-bsi-buktikemanan-siber-di-indonesia-lemah-dari-skala-satu-sampai-10-skornya-3?page=all diakses pada tanggal 26 Mei 2023.

[5] Muhammad Iqbal Fasya, "Manajemen Risiko Perbankan Syariah Indonesia", *Jurnal Studi dan Ekonomi Bisnis Islam,* Vol 1. No. 2, Desember 2016. 36-53

Permasalahan terkait manajemen risiko tercantum dalam Q.S Yusuf ayat 67 :[6]

وَقَالَ يٰبَنِيَّ لَا تَدْخُلُوْا مِنْۢ بَابٍ وَّاحِدٍ وَّادْخُلُوْا مِنْ اَبْوَابٍ مُّتَفَرِّقَةٍۗ وَمَآ اُغْنِيْ عَنْكُمْ

مِّنَ اللّٰهِ مِنْ شَيْءٍۗ اِنِ الْحُكْمُ اِلَّا لِلّٰهِۗ عَلَيْهِ تَوَكَّلْتُ وَعَلَيْهِ فَلْيَتَوَكَّلِ الْمُتَوَكِّلُوْنَ

> Artinya : Dia (Ya'qub) berkata, "Wahai anak-anakku, janganlah kamu masuk dari satu pintu gerbang, dan masuklah kamu dari pintu-pintu gerbang yang berbeda-beda. (Namun), aku tidak dapat mencegah (takdir) Allah dari kamu sedikitpun. (Penetapan) hukum itu hanyalah hak Allah. Kepada-Nyalah aku bertawakal (saja) dan hendaklah kepada-Nya (saja) orang-orang yang bertawakal (meningkatkan) tawakal(-nya)."

Maksud dari ayat tersebut menjelaskan bahwa manajemen risiko dalam perspektif islam ialah memberi dukungan usaha dalam mengurangi risiko, dan hanya melalui perintah Allah keputusan dapat diambil serta menjadi bagian dari penentu hasil. Dengan begitu, manajemen risiko dapat diartikan sebagai suatu strategi untuk meminimalisir terjadinya risiko-risiko seperti kejahatan yang ditimbulkan oleh serangan siber.

Oleh karena itu, menjadi begitu penting untuk fokus pada bidang manajemen risiko. Terlepas dari segala ancaman dan tantangan, semua pihak harus dapat berpartisipasi dalam pencegahan kebocoran data pada sektor perbankan syariah. Kemampuan untuk mengelola risiko merupakan komponen paling penting pada tata kelola perusahaan agar lebih bagus, sebab tidak semua risiko dapat dihindari. Keunggulan manajemen risiko di

[6] Kementrian Agama RI, *Al-Quran dan Terjemahannya*", (Jakarta: Lajnah Pentashihan Mushaf Al-Qur'an, 2024), 243.

era digitalisasi ini terletak pada orientasinya pada data untuk mengidentifikasi dan mengelola risiko siber, keamanan informasi, dan risiko lainnya yang berhubungan dengan kecanggihan teknologi informasi.[7]

Hal tersebut menunjukan bahwa relasi antara Bank Syariah dan risiko yang mungkin saja terjadi merupakan dua hal yang tidak dapat terpisahkan. Keberadaan kelompok Lock-Bit 3.0 adalah satu contoh permasalahan yang harus dihadapi dan dicegah oleh Bank Syariah, sebab jika tidak dihadapi sekaligus diselesaikan, maka Bank Syariah dianggap sebagai perusahaan yang tidak berani dalam mengambil keputusan dari adanya serangan siber. Oleh karena itu, penerapan manajemen risiko dalam perbankan syariah di Indonesia harus sesuai dengan skala, kompleksitas dan kemampuan Bank secara konsisten, sehat, dan sesuai dengan prinsip syariah. Perbankan syariah memerlukan sumberdaya yang mumpuni guna mengukur, mengidentifikasi risiko, dan mengembangkan teknik-teknik manajemen risiko.[8]

Beberapa penelitian yang sama terkait manajemen risiko juga pernah dilakukan, diantaranya yaitu oleh Yudi Herdian, Zen Munawar, dan Novianti Indah Putri, dalam penelitian tersebut memaparkan bahwa upaya melindungi adanya pencurian data, gangguan pada sistem informasi digital, dan sebagainya merupakan hal yang perlu untuk dilakukan sebagai suatu

---

[7] Mhd. Rizki Khairi, Muhammad Irwan Padli Nasution, dan Sri Suci Ayu Sundari. "Analisis Strategi Perbankan Syariah Menghadapi Manajemen Risiko di Era Digital". *Jurnal Ilmu Komputer, Ekonomi, dan Manajemen Vol. 2 No. 2, 2022.*

[8] Agustin, Hamdi, dan Hasrizal Hasan. "Teori Manajemen Risiko Bank Syariah". *Jurnal Tabarru': Islamic Banking and Finance 5, No. 2. 2022.* 551-564.

metode untuk mencegah kerugian. Adanya pandemi *Covid-19* juga menjadi faktor yang memungkinkan terjadinya risiko serangan siber. Risiko serangan siber termasuk sebagai risiko operasional terkait informasi dan aset teknologi yang bisa berdampak pada sebuah kerahasiaan, dan integritas pada sistem teknologi informasi (IT).[9] Risiko ancaman siber juga akan berdampak pada ketidakstabilan sistem keuangan utamanya pada sektor perbankan syariah, dsisi lain juga akan berdampak pada tingkat kepercayaan nasabah. Maka dalam hal ini peneliti memilih fokus penelitian terkait bagaimana penerapan manajemen risiko ysng dilakukan oleh Bank Syariah Indonesia.

Sektor perbankan syariah memiliki potensi dan prospek yang besar untuk terus berkembang dalam skala nasional maupun internasional, hal tersebut didukung oleh mayoritas pemeluk agama islam di Indonesia terbilang cukup besar, bahkan kinerja pada sektor perbankan syariah tercatat lebih unggul dari perbankan konvensional. Hal ini dapat diketahui berdasarkan data dari Otoritas Jasa Keuangan (OJK), yang menyebutkan bahwa pertumbuhan pembiayaan perbankan syariah pada Juni 2020 mencapai 10,13 persen, angka ini lebih tinggi dari penyaluran kredit dibanding perbankan konvensional yang sebesar 1,49 persen pada periode yang sama. Selain itu, pada sektor Dana Pihak Ketiga (DPK) perbankan syariah mencatat kenaikan yang begitu pesat mencapai 9 persen, sementara

[9] Yudi Herdiana, Zen Munwar, dan Novianti Indah Putri, "Mitigasi Risiko Keamanan Siber di Masa Pandemi *Covid-19*", *Jurnal ICT Information Communication & Technology, Vol. 21, No. 1, Juli 2017.* 42.

perbankan konvensional 7,95 persen. Dari sisi permodalan *Capital Aduadequacy Ratio* (CAR), perbankan syariah juga stabil di angka 21,20 persen. Rasio ini diatas kecukupan modal yang diatur oleh OJK sekitar 12-14 persen.[10]

Selain jumlah masyarakat muslim yang akan berpengaruh terhadap peningkatan nasabah, kemajuan tersebut juga didukung oleh adanya program Merger yang dilakukan oleh tiga Bank Syariah BUMN (Bank Mandiri Syariah, Bank BRI Syariah, dan Bank BNI Syariah), yang akan menciptakan efisiensi dalam hal penggalangan dana, operasional, pembiayaan, dan belanja. Artinya, program Merger turut menjadi faktor penunjang dalam perkembangan dan pertumbuhan perbankan syariah di Indonesia. Potensi Bank Syariah menjadi alternatif pilihan masyarakat Indonesia yang didukung oleh syariat agama Islam sekaligus berdampak baik dengan meningkatnya jumlah nasabah pada Bank Syariah. Lebih lanjut, kemungkinan hal buruk juga dapat terjadi berupa ancaman digital seperti peretasan dan pencurian data, maka perlunya kehati-hatian dan memperhatikan dalam hal perencanaan dan penetapan atas kebijakan secara transparan, efektif, efisien, dan rasional dengan tetap menghormati prinsip kebenaran.

[10] Nidya Waras Sayekti, Dkk. "Merger Bank Syariah Badan Usaha Milik Negara: *Quo Vadis?*", *Vol. 25, No. 3. Tahun 2020.* 233.

Dalam menghadapi meningkatnya serangan siber pada sektor perbankan, termasuk insiden yang pernah dialami Bank Syariah Indonesia (BSI), fokus terhadap keamanan digital menjadi semakin penting. Namun, pendekatan yang hanya menitikberatkan pada keamanan sistem *(cybersecurity)* cenderung bersifat reaktif dan teknis. Oleh karena itu, diperlukan kerangka kerja yang lebih strategis dan menyeluruh, yaitu manajemen operasional. Dengan pendekatan manajemen risiko, BSI dapat mengidentifikasi, menilai, dan mengendalikan potensi risiko siber tidak hanya dari sisi teknologi, tetapi juga dari dampaknya terhadap layanan, kepercayaan nasabah, reputasi syariah, dan keberlangsungan operasional. Selain itu, pendekatan ini juga sejalan dengan prinsip tata kelola risiko yang diatur oleh OJK dan prinsip kehati-hatian perbankan syariah.[11]

Di era digitalisasi yang semakin pesat, lembaga perbankan menghadapi tantangan baru dalam bentuk ancaman serangan siber *(cyber attack)* yang semakin kompleks dan canggih. Serangan siber tidak hanya berdampak pada aspek teknis seperti gangguan sistem atau pencurian data, tetapi juga menimbulkan risiko reputasi yang serius bagi institusi keuangan. Ketika terjadi serangan, bukan hanya sistem yang lumpuh, tetapi kepercayaan nasabah dan publik pun ikut tergerus.[12]

Serangan siber menjadi salah satu risiko utama dalam manajemen operasional bank modern. Ancaman seperti *ransomware, phishing,*

[11] Bank Indonesia, "Manajemen Risiko Keamanan Siber Bank Umum Departemen" (2021): 75.
[12] Ibid.

malware, hingga *Distributed Denial of Service* (DDoS) tidak hanya berpotensi mencuri data nasabah, tetapi juga dapat melumpuhkan sistem layanan inti perbankan. Ketika sistem terganggu atau bahkan lumpuh, proses bisnis menjadi terhambat, transaksi gagal dilakukan, dan kepercayaan nasabah terganggu semuanya masuk dalam kategori risiko operasional.

Menurut Peraturan OJK No. 18/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum. Risiko operasional adalah risiko akibat ketidakcukupan atau kegagalan proses internal, kesalahan manusia, sistem, atau dari kejadian eksternal. Serangan siber secara langsung masuk dalam klasifikasi ini, karena berpotensi menyebabkan gangguan sistem dan menimbulkan kerugian keuangan serta non-keuangan.[13]

Kasus serangan *ransomware* terhadap Bank Syariah Indonesia (BSI) pada Mei 2023 menjadi contoh nyata betapa seriusnya dampak serangan siber terhadap operasi bank. Selama beberapa hari, layanan BSI seperti mobile banking dan ATM mengalami gangguan, menyebabkan kelumpuhan sistem yang berdampak pada ribuan transaksi. Kantor cabang seperti BSI KCP Kediri Gudang Garam turut merasakan imbasnya, karena operasional menjadi terganggu dan layanan kepada nasabah tidak dapat berjalan normal.

[13] Otoritas Jasa Keuangan Indonesia, "PJOK No 18/POJK.03/2016," *Otoritas Jasa Keuangan* (2016): 1–29, http://www.ojk.go.id/id/kanal/iknb/regulasi/lembaga-keuangan-mikro/peraturan-ojk/Documents/SAL-POJK PERIZINAN FINAL F.pdf.

Kejadian tersebut menegaskan pentingnya integrasi manajemen risiko operasional yang adaptif terhadap ancaman siber. Bank tidak hanya harus memiliki sistem perlindungan teknologi, tetapi juga mekanisme respons insiden, pemulihan layanan, dan pelatihan karyawan agar dapat mengenali dan menanggulangi serangan siber secara cepat dan tepat. Dengan latar belakang ini, penelitian mengenai bagaimana bank, khususnya pada level kantor cabang seperti BSI KCP Kediri Gudang Garam, menerapkan manajemen risiko operasional dalam menghadapi serangan siber menjadi sangat relevan. Kajian ini diharapkan dapat memberikan gambaran strategis tentang kesiapan sistem, prosedur mitigasi, serta kontribusi manajemen risiko terhadap kelangsungan operasional dan perlindungan terhadap nasabah.

Penelitian ini memiliki kebaruan pada fokus kajian yang secara spesifik menganalisis manajemen risiko operasional dalam menghadapi ancaman *cybercrime* pada layanan digital Bank Syariah Indonesia. Tidak seperti kajian sebelumnya yang cenderung membahas aspek teknis keamanan siber, penelitian ini menempatkan serangan siber sebagai bentuk risiko operasional yang dapat mengganggu keberlangsungan layanan digital dan kepercayaan nasabah. Penelitian ini juga menggunakan pendekatan berbasis studi kasus insiden nyata (*cyberattack* terhadap BSI tahun 2023), serta mengintegrasikan perspektif tata kelola syariah dalam analisis risiko reputasi. Dengan demikian, penelitian ini diharapkan memberikan

kontribusi ilmiah dan praktis dalam memperkuat manajemen risiko di sektor perbankan syariah di Indonesia.

Mengingat Bank Syariah Indonesia KCP Kediri Gudang Garam merupakan salah satu cabang Bank Syariah Indonesia yang terletak di daerah dengan aktivitas ekonomi yang signifikan, khususnya di sektor industri dan perbankan. Kedua, lokasi ini memiliki infrastruktur digital yang cukup berkembang, sehingga menjadi representatif untuk mempelajari risiko *cybercrime* dalam konteks layanan perbankan digital. Ketiga, BSI KCP Kediri Gudang Garam telah menunjukkan komitmen dalam implementasi teknologi informasi dan keamanan siber, menjadikannya tempat yang tepat untuk mengevaluasi manajemen risiko dan strategi mitigasi yang diterapkan. Studi ini diharapkan dapat memberikan kontribusi dalam memperkuat sistem keamanan digital dan meningkatkan kesadaran terhadap ancaman *cybercrime* di sektor perbankan syariah. Berdasarkan alasan dan permasalahan diatas, maka peneliti tertarik untuk mengangkat fenomena yang terjadi pada Bank Syariah Indonesia. Dengan demikian, peneliti akan melakukan kajian penelitian yang berfokus pada penerpan manajemen risiko, dengan judul "Manajemen Risiko Dalam Menghadapi *Cybercrime* Pada Layanan Digital (Studi di Bank Syariah Indonesia KCP Kediri Gudang Garam)".

B. Fokus Penelitian

Berdasarkan konteks penelitian diatas, maka fokus penelitian ini adalah sebagai berikut:

1. Bagaimana *cybercrime* pada layanan digital di Bank Syariah Indonesia KCP Kediri Gudang Garam?
2. Bagaimana manajemen risiko dalam menghadapi *cybercrime* pada layanan digital di Bank Syariah Indonesia KCP Kediri Gudang Garam?

C. Tujuan Penelitian

Merujuk dari fokus penelitian diatas, maka tujuan penelitian yang akan dilakukan yaitu sebagai berikut:

1. Untuk menjelaskan bentuk-bentuk *cybercrime* pada layanan digital di Bank Syariah Indonesia KCP Kediri Gudang Garam.
2. Untuk menjelaskan manajemen risiko dalam menghadapi *cybercrime* pada layanan digital di Bank Syariah Indonesia KCP Kediri Gudang Garam.

D. Manfaat Penelitian

Bagian ini memuat manfaat yang akan ditimbulkan sesudah penelitian ini selesai dilaksanakan. Manfaat tersebut berupa manfaat secara teoritis maupun secara praktis.

Berikut adalah manfaat dari penelitian ini adalah:

1. Manfaat Teoritis

   Secara teoritis hasil dari adanya penelitian ini diharapkan mampu memberikan dorongan dalam proses mengembangkan ilmu, terlebih pada ilmu yang berkaitan dengan manajemen risiko ancaman siber pada layanan digital.

2. Manfaat Praktis

   Secara praktis hasil penelitian ini diharapkan mampu menjadi sumbangan pemikiran mengenai manajemen risiko ancaman siber terhadap sistem layanan digital bagi lembaga yang terkait, dan nasabah dari lembaga tersebut.

E. Penelitian Terdahulu

Berdasarkan penelusuran yang dilakukan penulis, beberapa penelitian serupa yang telah dilakukan sebelumnya yang berkesinambungan dengan permasalahan yang dibahas dalam penelitian ini. Peneliti menemukan ada beberapa literatur jurnal dan skripsi yang membahas tentang bahaya *cybercrime* pada layanan digital, diantaranya:

1. Penelitian yang dilakukan oleh Kukuh Dwi Kurniawan dan Dwi Ratna Indri Hapsari pada tahun 2021, dengan judul "Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah"[14]. Jurnal penelitian ini membahas tentang kewajiban bank untuk menjaga dan melindungi nasabahnya dari segala jenis kejahatan dalam dunia maya.

   Penelitian yang dilakukan dalam tinjauan ini didasarkan pada pendekatan hukum yang menggambarkan peraturan untuk melindungi nasabah bank dari kejahatan dunia maya. Referensi dalam jurnal ini adalah peraturan perundang-undangan yang berlaku di Indonesia yang memberikan gambaran normatif mengenai permasalahan cybercrime khususnya bagi nasabah bank, menggambarkan sifat kejahatan dan tantangan dalam penerapan hukum kejahatan itu sendiri di bidang teknologi informasi, serta sejauh mana undang-undang yang ada saat ini dapat memberikan perlindungan terhadap tindakan preventif dan represif, sehingga menjadi kerangka hukum penyelesaian kejahatan siber di sektor perbankan.

   Sebagai landasan hukun untuk melindungi nasabah atau konsumen dari kejahatan dunia maya peneliti merujuk pada Undang – Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

[14] Kukuh Dwi Kurniawan, Dwi Ratna Indri Hapsari, "Kejahatan Dunia Maya Pada Sektor Perbankan Di Indonesia: Analisa Perlindungan Hukum Terhadap Nasabah*", Jurnal ilmu hukum,* Vol 10, No, 2, Oktober 2021. 126-129.

(UUPK) pada Pasal 1 angka 1 menyebutkan bahwa “Perlindungan konsumen adalah segala upaya yang menjamin adanya kepastian hukum untuk memberi perlindungan kepada konsumen”. Bahwa Negara melalui berbagai sistem dan instrumen pelaksananya memberikan garansi dan kepastian hukum dengan memberikan perlindungan kepada konsumen di wilayah hukum Indonesia melalui upaya-upaya yang ditujukan untuk mencegah adanya ancaman pelaku usaha yang nakal atau tidak mau bertanggung jawab atas kegiatan usahanya tersebut dengan terciptanya kemudahan dalam memanfaatkan teknologi informasi pada aspek perbankan dengan baik sehingga tidak tercipta rasa takut atas tidak ada itikad baik dari para pelaku usaha dalam memberikan dan menjalankan kewajibannya atas hak yang harus diberikan kepada konsumen.

Persamaan pembahasan pada penelitian ini dengan penelitian yang akan dilakukan oleh peneliti yaitu, memiliki persamaan dalam pembahasan tentang kejahatan dunia maya yang terjadi pada sektor perbankan. Perbedaan penelitian ini dengan penelitian yang akan dilakukan yaitu pada lokasi penelitian, serta pada penelitian ini terfokus pada analisis landasan hukum yang ada di Indonesia sedangkan pada penelitian yang akan dilakukan yaitu terfokus pada penerapan manajemen risisko yang dilakukan oleh pihak perbankan secara langsung.

2. Penelitian ini dikakukan oleh Khabib Solihin & Fajar Adhi Kurniawan pada tahun 2022 dengan judul "Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman *Cyber Security*".[15] Penelitian ini menggunakan metode penelitian kualitatif, adapun objek pada penelitian ini yaitu pada KSPPS Artha Bahana Syariah Pati, dalam pengambilan data diperoleh dari *focus group discussion* dan wawancara mendalam dengan pimpinan KSPPS dan pejabat terkait.

   Penelitian ini membahas mengenai risiko ancaman keamanan siber khususnya pada layanan aplikasi berbasis Android dan Internet, dan hasil kajian menunjukkan bahwa penerapan manajemen risiko di KSPPS Artha Bahana Syariah terkait ancaman keamanan siber dicapai melalui pemantauan manajemen secara aktif dan kecukupan kebijakan. . . dan prosedur penggunaan teknologi informasi, kecukupan proses identifikasi, pengukuran, pengelolaan dan pemantauan risiko TI dan sistem pengendalian internalsaat menggunakan teknologi informasi.

   Persamaan penelitian ini dengan penelelitian yang akan dilakukan yaitu, menjadikan manajemen risiko ancaman kejahatan di bidang digital menjadi fokus yang ingin diteliti. Perbedaan

[15] Khabib Solihin & Fajar Adhi Kurniawan, *"*Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman *Cyber Security", Journal of Indonesian Sharia Economics,* Volume 1 Nomor 1 Maret 2022. 8.

penelitian ini dengan penelitian yang akan dilakukan yaitu terdapat pada objek penelitian.

3. Penelitian ini dilakukan oleh Edy Soesanto, Achmad Romadhon, Bima Dwi Mardika, Moch Fahmi Setiawan pada tahun 2023 dengan judul "Analisis dan Peningkatan Keamanan *Cyber:* Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File".[16] Dalam penelitian ini menggunakan pendekatan kualitatif dengan melakukan wawancara terhadap ahli keamanan *cyber,* pengguna internet, dan pihak terkait dalam lingkungan digital.

   Pembahasan dalam penelitian ini berfokus pada pencurian informasi dan data rahasia sebagai ancaman kejahatan dunia maya yang menyasar individu, lembaga pemerintah, dan angkatan bersenjata serta dapat membahayakan pertahanan suatu negara. Oleh karena itu, penting untuk mengelola risiko informasi dan komunikasi untuk mengurangi kerentanan terhadap penyalahgunaan informasi dan data di dunia maya, yang dapat berdampak pada banyak warga negara dan informasi rahasia. Selain pertahanan negara yang kuat, diperlukan juga dukungan hukum yang berjejaring dan saling mempengaruhi dalam menghadapi ancaman kejahatan siber.

[16] Edy Susanto, dkk, "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File"*, SAMMAJIVA : Jurnal Penelitian Bisnis dan Manajemen*, Vol.1, No.2 Juni 2023. 185.

Persamaan yang terdapat pada penelitian ini dengan penelitian yang akan dilakukan yaitu, pada poin manajemen risiko terhadap adanya ancaman *cyber crime*. Perbedaan yang terdapat pada penitian ini dengan penelitian yang akan dilakukan yaitu, pada objek penelitian.

4. Penelitian ini dilakukan oleh Eko Budi, Dwi Wira, Ardian Infantono pada tahun 2021 dengan judul "Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di Era *Society 5.0".*[17] Dalam penelitian ini menggunakan pendekatan kualitatif dan deskriptif analitis dengan teknik pengumpulan data menggunakan studi pustaka dari penelitian sebelumnya dan data sekunder lainnya.

   Pembahasan pada penelitian ini membahas bahwa saat ini Indonesia tengah dalam keadaan darurat *cyber security* dan sudah mencapai tahap memprihatinkan. Strategi *cyber security* yang harus dilakukan Indonesia untuk mewujudkan keamanan nasional di era *society 5.0*, adalah dengan: 1) *capacity building* pada semua stakeholder, 2) Pembentukan UndangUndang Khusus tentang Tindak Pidana Siber agar terwujud kepastian hukum untuk *cyber security* di Indonesia, 3) Peningkatan sumberdaya manusia dengan mendidik dan merekrut tenaga profesional yang memiliki integritas dan etika yang baik untuk mendukung penguatan *cyber security.* 4)

[17] Eko Budi1, Dwi Wira, Ardian Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0", *Prosiding SENASTINDO AAU* Volume 3, Tahun 2021. 223–234

Kerjasama stakeholder di dalam negeri melalui multi stakeholderism dan kerjasama internasional dalam pengembangan dan penguatan kapasitas kemampuan *cyber security* baik itu untuk infrastruktur, sarana prasarana maupun dalam pengembangan kemampuan sumberdaya dalam bidang *cyber security.*

Persamaan yang terdapat pada penelitian ini dengan penelitian yang akan dilakukan yaitu, pada poin *cyber crime,* dan terdapat pada jenis pendekatan yang dilakukan yaitu menggunakan pendekatan kualitatif dan deskriptif . Perbedaan yang terdapat pada penitian ini dengan penelitian yang akan dilakukan yaitu, pada objek penelitian dimana dalam penelitian ini masih bersifat global sedangkan dalam penelitian yang akan dilakukan mengerucut pada dunia perbankan yaitu pada Bank Syariah Indonesia.

5. Penelitian ini dilakukan oleh Muhammad Khairul Faridi pada tahun 2018 dengan judul "Kejahatan Siber Dalam Bidang Perbankan".[18] Dalam penelitian ini menggunakan metode kualitatif dengan pendekatan *library repository,* dikarenakan penelitian ini menggabungkan beberapa penelitian terdahulu yang terkait dengan siber di dunia perbankan.

   Pembahasan dalam penelitian ini adalah penerapan teknologi internet pada perbankan sangatlah penting. Sayangnya penggunaan

[18] Muhammad Khairul Faridi, "Kejahatan Siber Dalam Bidang Perbankan", *CyberSecurity dan Forensik Digital,* Vol. 1, No. 2, Desember 2018, 57-61

teknologi ini masih rentan terhadap aktivitas kriminal seperti skimming, hacking, dan malware. Oleh karena itu, diperlukan inovasi dalam sistem keamanan perbankan untuk melindungi dan memberantas kejahatan dalam transaksi elektronik. Penelitian terkait menunjukkan bahwa adasolusi berbeda untuk mengatasi masalah ini, termasuk menerapkan otentikasi tiga kali lipat, yaitu penggunaan kata sandi, token, dan data biometrik. Selain itu, keamanan juga dapat menggunakan data besar untuk memproses transaksi keuangan yang tidak wajar.

Persamaan dalam penelitian ini dengan penelitian yang akan dilakukan yaitu terdapat pada metode penelitian yaitu kualitatif, dan peneliian ini sama membahas tentag kejahatan siber dibidang perbankan. Perbedaan yang terdapat pada penelitian ini dengan penelitian yang akan dilakukan yaitu, pada objek penelitian dimana dalam penelitian ini masih bersifat global didalam dunia perbankan jadi sifatnya luas (konvensional atau syariah) sedangkan dalam penelitian yang akan dilakukan lebih mengerucut pada Bank Syariah Indonesia.