e-ISSN 2798-8260

Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora Vol: 5, No 1, 2025, Page: 1-9

Kajian Kriminologi: Mitigasi *Cyber Security* Sebagai Penanggulangan Serangan *Cyber Crime* dan Upaya *Recovery* (Studi Bank Sumsel Babel Syari'ah)

Abdul Rahman Ashidiq*, Lendra Dika Kurniawan, Ronaldi

Universitas Muhammadiyah Bangka Belitung

Abstrak: Penelitian ini menggunakan pendekatan kajian kriminologi terapan dengan perspektif teori Higiene Kriminal dan Politik Kriminal. Pendekatan ini bertujuan untuk melihat bagaimana bekerjanya *cyber security* sebagai upaya preventif dan represif dalam menanggulangi *cyber crime*. Tujuan penelitian ini untuk melihat dalam kajian Kriminologi sejauh mana *cyber security* di Bank Sumsel Babel Syari'ah dalam melakukan Mitigasi dari ancaman dan serangan *cyber crime* dan upaya *Recovery* ketika terjadi ancaman maupun serangan *cyber crime*. Metode Penelitian ini menggunakan kualitatif dengan cara melakukan olahan data dari hasil pengumpulan data yang diperoleh baik itu melalui observasi, studi dokumen maupun hasil wawancara. Hasil penelitian menunjukkan bahwa dalam mitigasi risiko, melalui kajian Higiene Kriminal upaya preventif yang dilakukan BSB Syari'ah dalam pencegahan terhadap kejahatan siber sudah sangat memadai, Sedangkan dalam upaya *recovery*/ pemulihan, melalui kajian Politik Kriminal upaya represif yang dilakukan BSB Syari'ah dengan mengoptimalkan tugas dari tim IT, yaitu tim Garda Siber dengan menjalankan kebijakan atau prosedur yang sudah dibuat dalam penanganan indikasi serangan siber, seperti melakukan pengisolasian, melakukan pemberantasan serta melakukan pemulihan sistem pasca terjadinya indikasi serangan siber.

Keywords: Kajian Kriminologi, Mitigasi *Cyber Security, Cyber Crime*

DOI: https://doi.org/10.53697/iso.v5i1.2315
*Correspondence: Abdul Rahman Ashidiq
Email:abdul.rahmanashidiq@unmuhbabel.ac.id

Received: 26-04-2025
Accepted: 26-05-2025
Published: 25-06-2025

Abstract: *This study uses an applied criminology study approach with the perspective of Criminal Hygiene and Criminal Politics theory. This approach aims to see how cyber security works as a preventive and repressive effort in overcoming cyber crime. The purpose of this study is to see in the Criminology study to what extent Cyber Security at Bank Sumsel Babel Syariah in Mitigating Cyber Crime threats and attacks and Recovery efforts when Cyber Crime threats or attacks occur. This research method uses qualitative by processing data from the results of data collection obtained either through observation, document studies or interview results. The results of the study show that in risk mitigation, through the Criminal Hygiene study, the preventive efforts carried out by BSB Syariah in preventing cyber crime are very adequate, while in recovery efforts, through the Criminal Politics study, the repressive efforts carried out by BSB Syariah by optimizing the tasks of the IT team, namely the Cyber Guard team by implementing policies or procedures that have been made in handling indications of cyber attacks, such as isolating, eradicating and restoring the system after an indication of a cyber attack occurs.*

Abstract: *Criminology Study, Cyber Security Mitigation, Cyber Crime*

Pendahuluan

Memanfaatkan kemajuan teknologi memang dibutuhkan di era sekarang ini baik di sektor perusahaan, sektor pemerintahan maupun sektor keuangan. Dalam sektor keuangan dapat membantu perbankan dan memudahkan bank dalam memberikan pelayanan dan informasi kepada masyarakat dengan memanfaatkan kemajuan teknologi. Misalkan dengan kemudahan bagi nasabah baru yang ingin bergabung dan membuka rekening cukup melakukan pendaftaran memalui online dengan *smartfone* masing-masing (Fauzi dkk, 2023).

Selain itu kemudahan dalam transaksi dengan menggunkan aplikasi mobile banking, kemudahan dalam penarikan tanpa kartu melalui ATM dan kemudahan penyimpanan yang saat ini cukup ke ATM bisa dilakukan tanpa harus langsung ke bank. Akan tetapi, dengan memanfaatkan kemajuan teknologi juga mengharuskan sektor perbankan waspada dan berhati-hati terhadap kejahatan yang juga memanfaatkan kecanggihan teknologi yaitu adanya *cyber crime* atau kejahatan siber (Parulina dkk, 2021).

Potensi terjadi Serangan siber atau kejahatan siber di sektor keuangan sangatlah besar, termasuk pada sektor perbankan yang disitu terjadi perputaran keuangan sangatlah masif, sehingga cukup menggiurkan bagi para pelaku kejahatan siber untuk berusaha mensabotase sistem keamanan perbankan demi mendapatkan keuntungan pribadi atau kelompok. Hal tersebut tentuanya selain akan merugikan pihak perbankan itu sendiri juga akan mengakibatkan kerugian bagi pihak nasabah karena adanya serangan *cyber crime*, sehingga mengakibatkan gangguan operasional sistem bank dan bahkan sampai terjadinya pencurian atau kebocoran data nasabah (Suwiknyo, 2021).

Seiring berkembangnya kecanggihan teknologi, maka berkembang pula cara-cara terjadinya serangan siber, bisa langsung menyerang server atau sistem keamanan Perbankan, misalnya berupa memasukan *malware* atau sejenis virus ke server Perbankan (Luthfah, 2024), guna untuk mencari celah atau kelemahan pada sistem keamanan Bank, atau juga bisa yang menjadi target langsung nasabah dari Perbankan (Azzahrah dkk, 2024), misalnya adanya *Phising* yang dilakukan oleh pelaku yang korban sasarannya adalah nasabah Bank, dengan cara menipu korban atau mengelabui korban untuk mendapatkan data-data pribadi korban, seperti pin ATM korban guna untuk memperoleh keuntungan pribadi atau dalam bentuk lainnya.

Tantangan yang kompleks dan upaya untuk menanggulangi adanya serangan siber di sektor perbankan bukanlah hal yang mudah untuk dilakukan. Meskipun demikian, pihak perbankan haruslah selalu waspada terhadap andanya indikasi serangan siber yang mengancam sistem keamanan siber. Oleh sebab itu pentinglah setiap bank baik itu bank milik BUMN, bank swasta, maupun bank-bank dibawah pemerintah daerah atau BUMD seperti Bank Sumsel Babel Syari'ah haruslah mempersiapkan *cyber security* yang kuat dan memadai. Bukan hanya itu, upaya mitigasi *cyber security* haruslah dilakukan sedini mungkin, begitu juga kecepatan recovery atau pemulihan pasca adanya serangan atau indikasi *cyber crime* (Dermawan dkk, 2023).

Tentunya mempersiapkan mitigasi *Cyber Security* atau keamanan siber bagi bagi Bank Sumsel Babel Syari'ah merupakan hal yang penting dan juga pada setiap sektor

instansi yang ada di Indonesia (Budi dkk, 2021). Begitu pula pada sektor yang menjalankan rotasi keuangan seperti Perbankan (Chirzah & Fadli, 2023). Istilah Keamanan (*security*) secara umum diartikan sebagai kemampuan mempertahan diri (*survival*) dalam menghadapi ancaman yang nyata (*existential threat*) (Munawarah & Yusuf, 2022). Sedangkan *Cyber security* merupakan upaya untuk memastikan pencapaian dan pemeliharaan sistem keamanan bagi setiap organisasi dan aset pengguna terhadap risiko serangan *Cyber Crime* (Ardiyanti, 2016).

Dalam kajian Kriminologi terapan/praktis seperti Higiene Kriminal memandang *Cyber Security*/keamanan siber merupakan upaya preventif untuk menanggulangi risiko adanya ancaman dan serangan *cyber crime* (Neubacher, 2023). Sedangkan kajian kriminologi terapan Politik Kriminal merupakan suatu usaha yang rasional dalam menanggulangi kejahatan yang terjadi, maka mitigasi *cyber security* tersebut sebagai upaya represif dalam melakukan recovery pada sistem keamanan siber yang diserang oleh *cyber crime* (Ida Rahma, 2018).

Berdasarkan paparan di atas, penelitian ini memuat rumusan masalah yaitu bagaimana kesiapan Bank Sumsel Babel Syari'ah terkait mitigasi *Cyber Security* sebagai penanggulangan serangan *Cyber Crime* dan upaya *Recovery* atau pemulihan pasca adanya atau indikasi serangan *cyber crime*.

Metodologi

Jenis penelitian ini merupakan penelitian kualitatif, dengan cara melakukan olahan data dari hasil pengumpulan data yang telah diperoleh baik itu melalui observasi, studi dokumen maupun hasil wawancara dan kemudian ditarik sebuah kesimpulan yang bersifat mendeskripsikan secara sistematis dan terstruktur (Ahmad & Muslimah, 2021).

Penelitian ini menggunakan pendekatan kajian kriminologi terapan yaitu menggunakan teori Higiene Kriminal dan Politik Kriminal. Melalui teori ini bertujuan untuk melihat bagaimana bekerjanya *cyber security* sebagai upaya preventif dan juga sebagai upaya represif dalam menanggulangi *cyber crime* (Agung dkk, 2023).

Objek dalam penelitian ini untuk mengetahui bagaimana sistem keamanan siber Bank Sumsel Babel Syari'ah dalam tinjauan ilmu kriminologi terapan/praktis sebagai upaya mitigasi dari serangan siber baik secara preventif maupun represif. Adapun pelaksanaan penelitian ini dilakukan dalam kurun waktu 3-6 bulan, mulai dari persiapan dan pendalaman materi hingga laporan akhir.

Pengumpulan data dengan cara mengidentifikasi masalah dengan melakukan pendalaman referensi, teori guna membantu dalam penyususan intrumen penelitian dan melakukan observasi secara online berkaitan dengan objek yang akan diteliti, selanjutnya melakukan kajian dan analisis dokumen dari hasil observasi yang didapatkan, dan melakukan wawancara kepada penanggungjawab atau kepada tim IT Bank Sumsel Babel Syari'ah (Malahati, 2023).

Hasil dan Pembahasan

A. Mitigasi risiko *cyber security* atau keamanan siber Bank Sumsel Babel Syari'ah

Sistem keamanan siber Bank Sumsel Babel Syari'ah saat ini berada dibawah naungan sistem keamanan siber kantor pusat Bank Sumsel Babel yang beralamat Jl. Gubernur H. Ahmad Bastari No. 7 Kel. Silaberabti Kec. Seberang Ulu I Jakabaring Palembang. Sedangkan semua sistem keamanan siber di Kantor Cabang BSB Syari'ah/Unit Usaha Syari'ah yang berada di wilayah Bangka Belitung seperti kantor cabang syari'ah yang beralamat di Jl. Jenderal Sudirman No, 23 di kota Pangkal Pinang dan kantor cabang pembantu syari'ah beralamat di Jl. Muhidin No. 135 yang terletak Sungaliat, saat ini terpusat hanya di kantor pusat Pelembang saja. Sehingga di kantor cabang syari'ah Pangkal Pinang dan Kantor Cabang Pembantu di Sungaliat hanya menjalankan kegiatan pelayanan operasional saja (https://www.banksumselbabel.com/id/page/10036/tim-garda-siber-bsb).

Dalam rangka mempersiapkan sistem keamanan siber yang mumpuni BSB membentuk tim khusus yang bertugas di bidang keamanan siber, yang diberi nama dengan Tim Tangggap Insiden Siber Bank Sumsel Babel yang kemudian juga dikenal dengan Tim Garda Siber BSB dan saat ini telah menjadi bagian dari Tim tanggap insiden siber nasional dibawah BSSN. Tugas dari dari Tim Garda Siber tersebut menangani insiden adanya gangguan sistem, gangguan keamanan informasi dan gangguan adanya indikasi serangan siber. Selain itu kemudahan untuk mengubungi Tim Garda Siber BSB dapat menggunakan email yaitu garda.siber@banksumselbabel.com (Putra, 2023).

Strategi selanjutnya yang dilakukan Bank Sumsel Babel untuk memitigasi risiko keamanan siber yaitu dengan penggunaan kontrol keamanan, audit keamanan berkala, dan melakukan program pelatihan karyawan.

Berdasarkan hasil wawancara dengan Novrizal Azhari, selaku analis risiko keamanan digital BSB, bahwa Bank Sumsel Babel menerapkan metode keamanan siber yang mengacu pada standar keamanan internasional, yaitu ISO 27001:2022 dan PCI DSS (*Payment Card Industry Data Security Standard*). Alasan Bank Sumsel Babel memilih metode keamanan siber yang mengacu pada ISO 27001:2022 dan PCI DSS karena keduanya merupakan standar internasional yang diakui untuk memastikan keamanan data dan transaksi perbankan.

Metode keamanan siber yang diterapkan oleh Bank Sumsel Babel bekerja dengan prinsip perlindungan berlapis untuk menjaga keamanan data dan transaksi perbankan, dimana aspek keamanan informasi terdiri dari keamanan pada aspek *People*, aspek Proses, dan aspek Teknologi.

Bank Sumsel Babel juga menjadwalkan audit secara berkala menggunakan auditor internal dan/ atau eksternal untuk memastikan semua sistem dan kontrol memenuhi standar. BSB melakukan audit internal setidaknya setiap tahun untuk meninjau kebijakan keamanan, kontrol akses, dan kepatuhan terhadap peraturan yang berlaku.

Selain itu juga BSB menggunakan auditor pihak ketiga setiap tahun untuk melakukan audit eksternal yang komprehensif. Hasil dari auditor eksternal dapat memberikan masukan secara objektif terhadap praktik keamanan dan membandingkannya dengan standar dan peraturan yang berlaku.

BSB Memiliki pegawai yang memiliki keahlian di bidang keamanan siber baik itu dari lulusan Teknik Informatika maupun karyawan yang dilatih dengan cara mengikuti pelatihan yang diselenggarakan oleh badan resmi seperti dari Kementerian Informasi, Badan Siber dan Sandi Negara maupun dari OJK. BSB juga mengembangkan pelatihan keamanan siber untuk semua karyawan yang berfokus pada topik seperti *phishing*, praktik kata sandi yang aman, dan penanganan informasi sensitif. BSB juga selalu melakukan pembahuruan materi pelatihan secara berkala sesuai dengan kebutuhan untuk mengatasi ancaman keamanan siber terkini.

Selain strategi di atas, Upaya preventif yang dilakukan oleh Bank Sumsel Babel dalam keamanan siber melibatkan langkah-langkah proaktif untuk melindungi sistem dan data nasabah. Seperti memastikan keamanan data sensitif dan mencegah akses tidak sah, kontrol keamanan seperti *firewall, enkripsi*, kontrol akses yang ketat, implementasi teknologi keamanan untuk pemantauan secara real-time guna mendeteksi dan memblock ancaman siber, serta memastikan tata kelola keamanan berjalan dengan baik.

Strategi yang lain juga seperti audit keamanan berkala dengan uji penetrasi juga dilakukan guna dapat membantu mengidentifikasi dan mengatasi kerentanan sistem keamanan siber yang dimiliki oleh BSB, sehingga dapat dilakukan perbaikan sistem keamanan siber yang dinilai berpotensi masuknya atau mendapatkan serangan siber.

Selanjutnya, Jika ditinjau melalui kajian kriminologi, bahwa mitigasi sistem keamanan siber yang dipersiapkan oleh BSB merupakan suatu upaya yang cukup matang sebagai pembenteng pencegahan dari kejahatan siber, karena salah satu objek dari kajian kriminologi selain mempelajari dengan cara mecari faktor atau penyebab terjadinya kejahatan siber, juga yang paling penting bagaimana menangani kejahatan siber yang kemungkinan akan terjadi, sehingga adanya upaya preventif tersebut sebagai pencegahan sejak dini terhadap kemungkinan adanya serangan siber, hal tersebut sejatinya telah dipersiapkan oleh BSB.

Teori Higiene Kriminal misalnya dapat membuka wawasan bahwa pentinya mitigasi/penanggulangan sejak dini dan pencegahan sebelum terjadinya kejahatan lebih baik dari pada pasca kejahatan itu terjadi baru ingin mencari solusi atau upaya untuk memberantas kejahatan, hal itu tentunya akan lebih sulit dan penuh dengan tantangan, apa lagi jika berkaitan dengan kejahatan siber yang notabennya sulit untuk di ketahui pelakunya siapa dan berada dimana, sehingga hampir sangat tidak mungkin jika hanya mengandalkan pelakunya ditangkap terlebih dahulu baru kemudian mencari solusi untuk menangani kasus kejahatan siber.

Salah satu penerapan Higiene Kriminal yang dilakukan BSB yaitu dengan membentuk Tim Garda Siber, yang bertugas sebagai garda terdepan untuk terus memantau dan juga menerima laporan jika adanya indikasi serangan siber ataupun gangguan terhadap sistem BSB, hal tersebut merupakan upaya pencegahan yang sangat efektif dan efesien. Efektif dalam arti jika dijumpai adanya indikasi serangan siber Tim Garda Siber dapat langsung mengatasi dengan cepet dan sigap. Sedangkan efesien dalam arti akan lebih memakan biaya yang lebih murah dan waktu yang tidak lama untuk mengatasi serangan siber karena dapat terdeteksi lebih awal.

Memperkuat pentinya penerapan Higiene Kriminal sebagai batasan untuk pencegahan terjadinya kejahatan siber, seperti kutipan salah satu ahli kriminologi yaitu Kaiser "bahwa membuat batasan dalam rangka pencegahan terhadap timbulnya kejahatan, merupakan suatu usaha yang meliputi atau mencakup segala tindakan, termasuk dalam hal ini tindakan mempersiapkan sistem keamanan siber yang mumpuni, dengan mempunyai tujuan khususnya untuk memperkecil luas lingkup dan terjadinya suatu kejahatan siber, baik melalui pengurangan kesempatan-kesempatan untuk melakukan kejahatan maupun melalui usaha-usaha preventif sebagai penanggulangan akan terjadinya kejahatan siber" (James, 2023).

Lebih lanjut, strategi yang dilakuan BSB seperti meningkatkan kontrol keamanan menggunakan *firewall*, *enkripsi* dan uji penetrasi dengan mengacu standar keamanan Internasional hal tesebut bagian dari penerapan Higiene Kriminal yaitu sebagai pencegahan primer. Dalam kriminologi pencegahan primer ditetapkan sebagai strategi pencegahan kejahatan melalui berbagai aspek atau bidang, termasuk bidang penguatan teknologi, hal itu dilakukan sebagai upaya intervensi atau campur tangan sebelum terjadinya kejahatan, dalam hal ini yaitu potensi adanya kejahatan siber (Zaidan, 2021).

Output yang sangat penting dari mempersiapkan dan penerapan metode keamanan siber seperti yang dilakukan BSB adalah terciptanya perlindungan data yang optimal serta terjaganya integritas dan kerahasiaan transaksi perbankan. Dengan mengacu pada standar internasional seperti ISO 27001:2022 dan PCI DSS, Bank Sumsel Babel berupaya memastikan kepatuhan terhadap regulasi yang berlaku, meningkatkan ketahanan terhadap ancaman siber, dan meminimalkan risiko kebocoran data.

2. Upaya *recovery* atau pemulihan Bank Sumsel Babel Syari'ah

Dalam penanganan recovery atau pemulihan dilakukan oleh Tim Tangggap Insiden Siber BSB dengan berkoordinasi kesemua unit/divisi yang ada di kantor BSB yang terkait, tergantung dengan kendala yang dialami. Hal yang paling penting dilakukan oleh tim IT dalam pemulihan sistem keamanan BSB yaitu pertama sebisa mungkin memulihkan sistem dan data dari cadangan yang telah disiapkan sebelumnya untuk memastikan bahwa informasi yang penting dapat dipulihkan tanpa kehilangan yang signifikan. Kedua melakukan verifikasi terhadap integritas sistem, memastikan bahwa tidak ada lagi jejak *malware* atau gangguan lainnya yang tersisa di dalam sistem. sKetiga mengembalikan operasi normal secara bertahap setelah melakukan pengujian yang cermat untuk memastikan bahwa sistem telah pulih sepenuhnya dan beroperasi dengan aman.

Jika terbukti terdeteksi adanya serangan siber upaya represif yang dilakukan BSB yaitu memiliki prosedur respon yang jelas dan cepat untuk menangani insiden tersebut.

Pertama tahap Pengisolasian, pada tahap ini tim IT BSB berfokus untuk menghentikan eskalasi insiden serta membatasi kerusakan lebih lanjut untuk menjaga kestabilan sistem keamanan. Hal yang dilakukan yaitu, Melakukan isolasi sistem yang terkena dampak dengan memutuskan koneksi jaringan untuk mencegah pergerakan yang dilakukan oleh pelaku kejahatan siber, Membatasi adanya pergerakan lalu lintas (*traffic*) yang berpotensi berbahaya, Pencabutan akses dengan mennonaktifkan akun pengguna

atau hak akses yang terinfeksi untuk membatasi aktivitas penyerang. Jika diperlukan melakukan penghentian layanan atau proses tertentu sesuai dengan jenis insiden yang terjadi. Serta Memberikan informasi kepada tim tanggap insiden internal dan pemangku kepentingan tentang kebocoran data tersebut untuk memastikan upaya penanggulangan yang terkoordinasi.

Kedua tahap Pemberantasan, pada tahap pemberantasan atau pembersihan dalam tanggap insiden merupakan upaya yang berfokus untuk menghilangkan akar penyebab dari kejadian keamanan yang terjadi dan mencegah kejadian serupa di masa depan. Pada tahap ini, tim IT BSB melakukan beberapa tindakan penting, diantaranya mengidentifikasi dan menghapus semua *malware* atau perangkat lunak berbahaya di sistem yang terinfeksi. Menggunakan *anti-malware* dan antivirus dan memastikan semua sistem dipindai, bukan hanya sistem yang awalnya terkena dampak. Memperbaiki kerentanan keamanan yang telah dieksploitasi oleh penyerang, untuk mencegah kejadian serupa terulang. Melakukan perbaikan sesuai dengan tingkat risiko kerentanan yang terekspos. Memperkuat konfigurasi sistem dan pengaturan keamanan untuk meningkatkan postur keamanan secara keseluruhan. Melakukan serangkaian pengujian untuk memastikan malware telah dihapus sepenuhnya dan sistem dikembalikan kekondisi aman sebelum menghubungkannya kembali ke jaringan.

Ketiga tahap Pemulihan sistem dan data, Pada tahap ini berfokus untuk mengembalikan sistem dan data yang terpengaruh ke kondisi fungsional serta memastikan sistem sudah beroperasi normal dan aman untuk digunakan kembali. Berikutnya BSB akan Melakukan Edukasi *Awareness* untuk memitigasi serangan berkelanjutan, serta yang tidak kalah penting adalah memastikan Backup layanan pada *Disaster Recovery Center* dapat berjalan selama proses pemulihan untuk memastikan layanan bank tetap beroperasional.

Selanjutnya, peninjauan melalui kajian kriminologi praktis politik kriminal sebagai upaya represif untuk mengatasi setelah terjadinya kejahatan, seperti yang dilakukan BSB saat ini yaitu melalui pendekatan reaksi informal. Dalam khasanah kriminologi, rekasi informal dapat dilakukan dan ditangani oleh masyarakat atau pihak yang menjadi korban dari kejahatan itu sendiri. Hal itu juga dikenal sebagai tindak kontrol sosial informal.

Hal yang serupa saat ini dilakukan oleh BSB, upaya represif lebih menekankan kepada pendekatan informal sebagai bentuk kontrol yang dilakukan secara internal, yaitu dengan menetapkan sebuah konseptual maupun behavioral. Dikatakan konseptual karena apa yang dilakukan oleh BSB difokuskan pada sikap internal dan persepsi internal dengan mengadepankan pengawasan sistem keamanan secara internal. Dikatakan bihavioral karena apa yang dilakukan BSB difokuskan pada usaha nyata dan aktual untuk mengatasi kejahatan siber secara rill (Djanggih, 2018).

Meskipun demikian, jika memang diperlukan BSB juga berkomitmen untuk mengatasi kejahatan siber melalui upaya represif melalui pendekatan formal, yaitu berkoordinasi dengan pihak eksternal, dalam hal ini yaitu pemerintah indonesia melalui OJK dengan tetap mematuhi arahan yang dikeluarkan oleh OJK berkaitan dengan Pedoman Keamanan Siber Bagi Penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK). Selain itu jika memang diperlukan, BSB juga akan berkoordinasi dengan pihak penegak hukum,

kementerian komdigi dan juga badan siber dan sandi negara khususnya untuk melakukan invenstigasi terkait penyebab terjadinya serangan dan mendeteksi siapa pelaku dari kejahatan siber.

Simpulan

Dalam mitigasi risiko, melalui kajian Higiene Kriminal upaya preventif yang dilakukan BSB Syari'ah dalam pencegahan terhadap kejahatan siber sudah sangat memadai, yaitu dengan cara sistem keamanan siber BSB Syari'ah saat ini menginduk dibawah naungan BSB kantor pusat, BSB Syari'ah juga membentuk Tim Garda Siber yang bertugas sebagai pengawas dan tim yang menangani jika adanya serangan siber, selain itu, BSB Syari'ah juga meningkatkan kontrol keamanan tingkat lanjut yang berstandar Internasional, melakukan audit keamanan berkala dan melakukan program pelatihan berkala.

Sedangkan dalam upaya *recovery*/pemulihan, melalui kajian Politik Kriminal upaya represif yang dilakukan BSB Syari'ah dengan mengoptimalkan tugas dari tim IT, yaitu tim Garda Siber dengan menjalankan kebijakan atau prosedur yang sudah dibuat dalam penanganan indikasi serangan siber, seperti melakukan pengisolasian, melakukan pemberantasan serta melakukan pemulihan sistem pasca terjadinya indikasi serangan siber.

Daftar Pustaka

Agung, A. H., Hafrida, & Erwin, E. (2023). Pencegahan Kejahatan Terhadap *Cyber crime*. Pampas J. Crim. Law, vol. 3, no. 2, pp. 212–222, doi: 10.22437/pampas.v3i2.23367.

Ahmad &Muslimah. (2021). Memahami Teknik Pengolahan dan Analisis Data Kualitatif. Proceedings, vol. 1, no. 1, pp. 173–186.

Ardiyanti, H. (2016). *Cyber-security* dan tantangan pengembangannya di indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 5(1).

Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). Tinjauan Literatur Tentang Ancaman *Cyber crime* Dan Implementasi Keamanan Siber Di Industri Perbankan. Humanitis: Jurnal Homaniora, Sosial dan Bisnis, 2(7), 692-700.

banksumselbabel.com. Tim Garda Siber. Diakses pada hari Selasa tanggal 31 Desember 2024, jam 15.34 WIB. Dari https://www.banksumselbabel.com/id/page/10036/tim-garda-siber-bsb

Budi E, D. Wira, and A. Infantono. (2021). Strategi Penguatan *Cyber Security* Guna Mewujudkan Keamanan Nasional di Era *Society* 5.0, Pros. Semin. Nas. Sains Teknol. dan Inov. Indones., vol. 3, no. November, pp. 223–234, doi: 10.54706/senastindo.v3.2021.141.

Chirzah, D. and E. Y. Al-fadli. (2023). Analisis Evaluasi Kebijakan Pada *Cyber Security* Perbankan, J. Trends, vol. 01, no. 01, pp. 19–24, [Online]. Available: https://ejurnal.ibisa.ac.id/index.php/jsd/article/view/290/27.

Dermawan, I., Baidawi, A., Iksan, & Mellyana Dewi, S. (2023). Serangan Cyber dan Kesiapan Keamanan *Cyber* Terhadap Bank Indonesia. Jurnal Informasi Dan Teknologi, 5(3), 20-25. https://doi.org/10.60083/jidt.v5i3.364.

Djanggih, H., & Qamar, N. (2018). Penerapan teori-teori kriminologi dalam penanggulangan kejahatan siber (*cyber crime*). *Pandecta Research Law Journal*, *13*(1), 10-23.

Fauzi, A. A., Kom, S., Kom, M., Budi Harto, S. E., Mm, P. I. A., Mulyanto, M. E., ... & Rindi Wulandari, S. (2023). Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa *Society* 5.0. PT. Sonpedia Publishing Indonesia.

James, G. (2023). *Pengantar Kriminologi*. Gilad James *Mystery School*.

Luthfah, D. (2024). Penguatan Keamanan Siber Pada Sektor Jasa Keuangan Indonesia. *Jurnal Penelitian Dan Karya Ilmiah Lembaga Penelitian Universitas Trisakti*, 259-267.

Malahati, F, A. U. B, P. Jannati, Q. Qathrunnada, & Shaleh, S. (2023). Kualitatif : Memahami Karakteristik Penelitian Sebagai Metodologi, J. Pendidik. Dasar, vol. 11, no. 2, pp. 341–348, doi: 10.46368/jpd.v11i2.902.

Munawarah, H. & M. Yusuf. (2022). Bank Digital Syariah Analisis *Cyber Security* Menurut Hukum Positif Di Indonesia Dan Hukum Ekonomi Syariah, vol. 8, no. 2.

Neubacher, F. (2023). Kriminologie. doi: 10.5771/9783748933601.

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies* (*Telnect)*, 1(2), 85-92.

Putra, H. Y. (2023) Perancangan Tim Siap Tanggap Insiden *Sibercsirt*: Studi Kualitatif Berdasarkan *Business Impact Analysis* Di Bank Sumsel Babel. *Masters Thesis*, Universitas Bina Darma.

Rahma, I. (2018). Penerapan Teori Dan Kebijakan Kriminal Dalam Pertimbangan Hukum Dalam Sistem Peradilan Pidana, At-Tasyri' J. Ilm. Prodi Muamalah, pp. 51–70, doi: 10.47498/tasyri.v10i2.212.

Suwiknyo, F. B. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. Lex Privatum, 9(4).

Zaidan, M. A., & Sh, M. (2021). Kebijakan Kriminal. Sinar Grafika (Bumi Aksara).