Volume 1 Nomor 1 Maret 2022
https://journal.ipmafa.ac.id/index.php/jiose
DOI: https://doi.org/10.35878/jiose.v1i1.360
e-ISSN: 2829-1719, ISSN: 2962-3812

Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman *Cyber Security*

Khabib Solihin[1] & Fajar Adhi Kurniawan[2]
Institut Pesantren Mathali'ul Falah
[1]Email korespondensi: khabib@ipmafa.ac.id; [2]Email: fajaradhi@ipmafa.ac.id

Abstrak
Penelitian ini adalah penelitian kualitatif yang membahas tentang penguatan manajemen risiko lembaga keuangan syariah non bank, KSPPS Artha Bahana Syariah Pati Jawa Tengah. Sumber data dalam penelitian ini diperoleh melalui *focus group discussion* dan wawancara mendalam dengan pimpinan KSPPS dan pejabat terkait. KSPPS Artha Bahana Syariah Pati Jawa Tengah mengembangan layanan digital berbasis internet kepada anggotanya dalam bentuk ABS *Mobile*. Penggunaan teknologi digital dan internet untuk meningkatkan layanan kepada anggota serta untuk memperoleh efektivitas dan efisiensi bisnis harus dilakukan disertai dengan penguatan manajemen risiko untuk mengantisipasi ancaman *cyber security*. Dari hasil penelitian menunjukkan bahwa penerapan manajemen risiko di KSPPS Artha Bahana Syariah terkait dengan ancaman *cyber security* dalam bentuk pengawasan aktif oleh pimpinan, kecukupan kebijakan dan prosedur penggunaan teknologi informasi, kecukupan proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko teknologi informasi, dan sistem pengendalian internal atas penggunaan teknologi informasi.
Kata kunci: Manajemen Risiko, KSPPS Artha Bahana Syariah, *Cyber Security*.

Abstract
This research is a qualitative research that discusses the strengthening of risk management non-bank Islamic financial institutions, KSPPS Artha Bahana Syariah Pati Central Java. The sources of data in this study were obtained through focus groups and in depth interviews with KSPPS leaders and related officials. KSPPS Artha Bahana Syariah Pati Central Java develops internet-based digital services to its members in the form of ABS Mobile. The use of digital and internet technology to improve services to members and to gain business effectiveness and efficiency must be accompanied by strengthening risk management to anticipate cyber security threats. The results of the study indicate that the application of risk management at KSPPS Artha Bahana Syariah is related to the threat of cyber security in the form of active supervision by the leadership, the adequacy of policies and procedures for the use of Information Technology, the adequacy of the identification, measurement, control, and monitoring of information technology risks, and the internal control system. on the use of information technology.
Keywords: Risk Management, KSPPS Artha Bahana Syariah, Cyber Security.

A. Pendahuluan

Penggunaan Teknologi Informasi dan Komunikasi (TIK) oleh rumah tangga di Indonesia lima tahun terakhir menunjukkan perkembangan yang pesat. Badan Pusat Statistik dalam Statistik Telekomunikasi Indonesia 2019 merilis data untuk persentase penduduk yang menggunakan telepon selular hingga pada tahun 2019 mengalami peningkatan mencapai 63,53%. Pertumbuhan penggunaan telepon selular tersebut diikuti oleh pertumbuhan kepemilikan komputer dan kepemilikan akses internet dalam rumah tangga yang mencapai angka 18,78% untuk kepemilikan komputer dan 73,75% untuk kepemilikan akses internet dalam rumah tangga. Lebih lengkapnya Badan Pusat Statistik menyajikan data bahwa penggunaan internet juga mengalami peningkatan selama kurun waktu 2015-2019, data tersebut ditunjukkan dari meningkatnya persentase penduduk yang mengakses internet pada tahun 2015 sekitar 21,98% menjadi 47,69% pada tahun 2019 (BPS, 2019).

Peningkatan penggunaan internet juga ditunjukkan pada kuartal II/2020 yang mencapai 196,7 juta atau 73,7% dari populasi. Jumlah ini bertambah sekitar 25,5 juta pengguna dibandingkan tahun sebelumnya. Peningkatan penggunaan teknologi internet ini didasari oleh banyak faktor diantaranya sebagaimana yang disampaikan oleh Ketua Umum Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) Jamalul Izza yang mengatakan bahwa kenaikan didorong oleh kehadiran infrastruktur internet cepat yang semakin merata dan transformasi digital yang masif akibat pandemi Covid-10 sejak Maret 2020 (teknologi.bisnis.com, 2020).

Peningkatan penggunaan teknologi internet di masyarakat sebagaimana data yang disajikan merupakan peluang besar yang harus ditangkap dan ditindaklanjuti oleh pelaku bisnis. Di samping sebagai peluang peningkatan gaya hidup masyarakat yang berbasis digital juga merupakan tantangan nyata untuk semua pelaku bisnis terutama terkait dengan kemampuan sumber daya internal perusahaan dalam memanfaatkan dunia digital untuk memenuhi kebutuhan konsumen sesuai dengan gaya hidupnya. Transformasi dan inovasi

bisnis dari layanan manual menuju layanan digital sangat dibutuhkan agar kebutuhan konsumen yang serba berbasis digital dapat terpenuhi serta perusahaan bisa mencapai kelangsungan hidupnya. Hal ini perlu dilakukan oleh semua sektor bisnis tidak terkecuali lembaga jasa keuangan syariah. Lembaga jasa keuangan syariah yang notabene merupakan bisnis yang bergerak dalam layanan jasa memiliki tantangan besar untuk selalu bertransformasi dan berinovasi dalam persaingan layanan digital untuk memenuhi kebutuhan penggunanya yang memiliki tuntutan serba cepat dan efisien dalam bertransaksi.

Hadirnya *internet banking, mobile banking, financial technologi*, serta transaksi lainnya yang berbasis digital menunjukkan bahwa saat ini lembaga jasa keuangan syariah sebagai penyedia jasa layanan transaksi keuangan untuk masyarakat terus melakukan inovasi berbasis digital untuk memenuhi kebutuhan masyarakat dan memenangkan persaingan global. Penguasaan teknologi serta kemampuan belajar dan berinovasi dengan teknologi saat ini menjadi salah satu modal besar untuk lembaga jasa keuangan syariah agar dapat bertahan dari persaingan dan mendapatkan keuntungan kompetitif dalam bisnisnya.

Media layanan digital seperti *internet banking, mobile banking, financial technologi* terbukti telah memberikan manfaat besar dalam perkembangan layanan keuangan untuk masyarakat, di antara manfaat besar yang diperoleh dari layanan digital adalah: *pertama,* layanan keuangan lebih inklusif dimana layanan keuangan bisa meluas tanpa harus membangun kantor cabang, termasuk mempekerjakan teller satpam serta pegawai lainnya. *Kedua,* layanan digital memberikan efisiensi layanan 24 jam. *Ketiga,* efisiensi biaya administrasi yang diakibatkan dari menurunnya biaya operasional lembaga keuangan (Kompas.com, 2021). *Keempat,* efektivitas layanan yang memudahkan pengguna dalam melakukan pembukaan buku rekening, transaksi keuangan, registrasi, komunikasi, dan penutupan rekening (Izma Fazlun Jannah, dkk., 2020). Manfaat yang dihasilkan oleh layanan digital lembaga keuangan terbukti dapat meningkatkan kepuasan pengguna, sebagaimana hasil penelitian yang

dilakukan oleh Lilis Susilawati dkk. (2020) yang menyimpulkan bahwa inovasi perbankan digital berpengaruh signifikan terhadap kepuasan nasabah perbankan (Lilis Susilawati & Nicola-Nocola, 2020).

Di samping manfaat besar yang melekat dalam pemanfaatan digital layanan jasa lembaga keuangan, ada risiko besar yang mengancam terutama terkait dengan kejahatan dalam dunia digital ketika lembaga keuangan berinovasi dalam layanan digital. Salah satu kasus yang mencuat pada awal tahun 2020 terkait dengan layanan digital lembaga keuangan adalah kasus pembobolan *m-banking* seorang wartawan senior dengan kerugian sebesar 1,12 milyar. Berdasarkan penyelidikan kepolisian, kasus pembobolan ini berasal dari data Sistem Layanan Informasi Keuangan (SLIK) korban. Data SLIK dijual oknum pegawai bank kepada komplotan pelaku kejahatan, bermodalkan data tersebut pelaku membuat Kartu Tanda Penduduk (KTP) palsu kemudian mengajukan permohonan pergantian SIM Card kepada operator telekomunikasi dengan alasan ponsel hilang. Setelah mendapatkan SIM card baru pelaku masuk ke email pribadi dan membobol email dengan memanfaatkan *one time password* (OTP). Selanjutnya melalui akses email pelaku berhasil mengganti password *m-banking* (cnbc indonesia.com, 2021).

Kasus lainnya yang pernah terjadi terkait dengan layanan digital lembaga jasa keuangan adalah pembobolan kartu kredit yang terkoneksi dengan *internet banking* dengan kerugian sebesar 1,11 milyar yang terjadi pada tahun 2019. Modus yang mendasari kasus ini adalah kartu SIM milik korban yang terhubung dengan internet banking telah lama nonaktif. Hal tersebut dimanfaatkan oleh para tersangka dengan cara mengaktifkan kembali kartu SIM tersebut sehingga otomatis akun *internet banking* milik korban juga kembali aktif. Sehingga *internet banking* yang sudah mati tersebut akhirnya aktif kembali dengan atas nama korban, pelaku kemudian menggunakan layanan kartu kredit melalui *internet banking* untuk pembelian online (cnnindonesia.com, 2021).

Kedua kasus tersebut menunjukkan bahwa keberadaan sistem, data, jaringan, dan program dalam layanan digital harus dilindungi dan tetap terjaga

kerahasiaannya. Kasus pembobolan *internet banking* serta *mobile banking* merupakan bukti konkrit dari ancaman *cyber security,* yakni ancaman keamanan atau serangan digital terhadap perlindungan sistem, data, jaringan, dan program. Selain kasus pembobolan *internet banking* serta *mobile banking* banyak modus kejahatan digital lain yang terkait dengan ancaman *cyber security*. Dilihat dari aktivitasnya, jenis-jenis ancaman *cyber security (cybercrime)* di antaranya *carding*, *hacking, cracking, defacing, phising*, *spamming* dan *malware.* Sedangkan dari modus operasinya ancaman *cyber security* di antaranya adalah *unauthorized access to computer system and service, illegal contents*, *data forgery, cyber espionage, cyber sabotage and extortion*, *offense against intellectual property*, dan *infringements of privacy* (Sulisrudatin, 2018).

Banyaknya ancaman *cyber security* dalam dunia digital sebagaimana yang disebutkan menunjukkan bahwa pemanfaatan teknologi digital dalam layanan lembaga jasa keuangan memposisikan sistem, data, jaringan serta program *(software)* sebagai modal besar yang harus dijaga. Kerentanan sistem, data, jaringan serta program terhadap peretasan merupakan masalah pokok yang tidak boleh diabaikan agar bebas dari ancaman *cyber security* serta merugikan masyarakat sebagai pengguna jasa. Usaha yang bisa dilakukan oleh lembaga keuangan untuk mengantisipasi ancaman *cyber security* adalah dengan memperkuat manajemen risiko dalam pemanfaatan layanan digital, hal ini dilakukan agar lembaga keuangan mampu mengambil peluang dan manfaat besar yang ada dalam pemanfaatan digital sekaligus meminimalisir terjadinya potensi risiko yang terkait dengan kejahatan dalam dunia digital untuk meminimalisir kerugian dan menjaga keamanan dana serta kenyamanan layanan jasa keuangan kepada pengguna.

Salah satu Lembaga Keuangan Syariah Non Bank di Kabupaten Pati yang telah memanfaatkan peluang teknologi serta menerapkan manajemen risiko terkait dengan ancaman *cyber security* adalah KSPPS Artha Bahana Syariah Pati. Layanan ABS Mobile merupakan salah satu layanan berbasis digital yang diberikan oleh KSPPS Artha Bahana Syariah kepada anggotanya dengan fasilitas *online* 24 jam. Adanya layanan online berbasis android ini tentu

memberikan manfaat besar kepada anggota terutama untuk fleksibilitas transaksi, akan tetapi tentu layanan ini tidak terlepas dari ancaman kejahatan digital salah satunya yang pernah terjadi di Tahun 2019 dimana beberapa user anggota diretas dan dipergunakan oleh orang-orang yang tidak bertanggung jawab untuk melakukan transaksi.

Berangkat dari kasus ini KSPPS Artha Bahana Syariah segera merespon permasalahan tersebut salah satunya dengan memblokir semua akun nasabah sehingga kurang dari 12 jam semua akun anggota dapat diamankan dan kerugian tidak lebih dari dua juta rupiah. Pasca kejadian tersebut KSPPS Artha Bahana Syariah meningkatkan keamanan sistem untuk kembali memberikan layanan yang efektif, efisien, serta aman kepada seluruh anggotanya melalui ABS Mobile. KSPPS Artha Bahana Syariah telah berproses dan melalui hal penting kaitannya dengan pemanfaatan teknologi digital, dalam perjalanannya KSPPS Artha Bahana Syariah mampu memanfaatkan teknologi digital untuk meningkatkan layanan kepada anggotanya sekaligus meminimalisir risiko yang terkait dengan teknologi digital.

Pencapaian yang didapat oleh KSPPS Artha Bahana Syariah tersebut perlu untuk diteliti dan dipublikasikan agar terdokumentasikan dan dapat menjadi salah satu referensi yang dapat digunakan sebagai rujukan oleh lembaga keuangan syariah lainnya di wilayah Kabupaten Pati untuk meningkatkan layanan berbasis digitalnya. Maka dari itu atas dasar latar belakang tersebut penelitian model penguatan manajemen risiko lembaga jasa keuangan non bank dalam menghadapi ancaman *cyber security* studi kasus di KSPPS Artha Bahana Syariah telah dilakukan dengan hasil sebagaimana yang diuraikan dalam artikel penelitian ini.

B. Metode Penelitian

Jenis penelitian ini adalah penelitian kualitatif, dimana jenis penelitian ini digunakan untuk meneliti pada kondisi objek yang alamiah. Dalam penelitian kualitatif ini peneliti sebagai instrumen kunci dengan analisis data yang bersifat kualitatif dan hasil yang lebih menekankan makna daripada generalisasi (Sugiyono, 2009). Penelitian ini juga masuk dalam kategori penelitian kancah

(Suharsimi Arikunto, 2014) atau penelitian lapangan *(field research)*. Tempat atau objek yang diambil dalam penelitian ini adalah KSPPS Artha Bahana Syariah Pati. Sumber data dalam penelitian ini diperoleh langsung oleh peneliti melalui *focus group* dan wawancara dengan General Manajer KSPPS Artha Bahana Syariah Pati serta pejabat terkait termasuk tim IT dan kepala bagian operasional.

Setelah data ditemukan dari sumber data melalui berbagai teknik, maka tahapan selanjutnya yang dilakukan peneliti adalah melakukan analisis data. Analisis data kualitatif adalah upaya yang dilakukan dengan jalan bekerja dengan data, mengorganisasi data, memilah-milahnya menjadi satuan yang dapat dikelola, mensintesiskan, mencari dan menemukan pola, menemukan apa yang penting dan apa yang dipelajari, dan memutuskan apa yang dapat diceritakan kepada orang lain (Lexi J. Moleong, 2008). Penelitian ini menggunakan teknik analisis yang ditawarkan oleh Miles dan Huberman (Sugiyono, 2009). Ada tiga tahap analisis yang dilakukan dalam penelitian ini yaitu reduksi data *(data reduction)*, penyajian data *(data display)* dan verifikasi *(conclusion drawing)*.

C. Hasil dan Pembahasan

1. Teknologi Digital KSPPS Artha Bahana Syariah dan Kasus Ancaman *Cyber Security*

Perkembangan teknologi digital memberikan dampak besar terhadap perkembangan semua sektor bisnis terutama dalam bidang keuangan. teknologi digital dalam perkembangan bisnis merupakan salah satu peluang besar sekaligus tantangan yang dihadapi oleh lembaga keuangan. Menjadi peluang besar karena teknologi digital mampu menghadirkan efektivitas dan efisiensi layanan, menjadi tantangan karena dibutuhkan kerja keras dan modal besar dalam membangun layanan berbasis digital di sebuah lembaga keuangan syariah. Terutama yang terkait dengan kesiapan sumber daya manusia dan komponen lainnya yang dibutuhkan.

Terlepas dari posisinya yang menjadi peluang ataupun tantangan, Rika Mawarni, dkk. (2021) dalam penelitiannya menjelaskan bahwa digitalisasi

produk dan layanan lembaga keuangan harus dilakukan dengan cepat dan responsif. Penerapan teknologi digital akan mengikuti teori ekonomi yang menjelaskan bahwa kemajuan teknologi mengarah pada peningkatan produktivitas dan mendorong efisiensi perusahaan. Perusahaan yang efisien dan produktif akan meningkatkan kemampuannya untuk bersaing dan mendominasi pasar (Rika Mawarni, dkk. (2021).

Pentingnya pengembangan layanan berbasis digital di lembaga keuangan syariah tentu dipahami oleh semua pelaku usaha. Begitu juga yang terdapat di KSPPS Artha Bahana Syariah Pati. Strategi pengembangan layanan yang dilakukan oleh KSPPS Artha Bahana Syariah terdiri dari pengembangan produk, perluasan jaringan kantor, dan pengembangan layanan digital. Terkait dengan pengembangan layanan berbasis teknologi digital di KSPPS Artha Bahana Syariah di antaranya adalah sebagai berikut;

Pertama, pengembangan teknologi yang terkait dengan sistem *core* (sistem operasional), pengembangan teknologi ini memungkinkan keterhubungan antar kantor dalam satu server melalui jaringan internet. Sehingga dengan adanya teknologi ini memungkinkan semua anggota untuk bertransaksi di semua kantor (tidak harus di kantor lokasi tempat dibukanya rekening) dan secara *real time* akan tercatat di rekening anggota. KSPPS Artha Bahana Syariah menggunakan sistem *core* SQL Database Visual FoxPro.

Kedua, pengembangan layanan berbasis internet dan aplikasi android. Kategori kedua ini diwujudkan oleh KSPPS Artha Bahana Syariah dalam bentuk layanan ABS Mobile. Layanan ini memberikan kemudahan dan fleksibilitas kepada anggota untuk melakukan transaksi secara *online* dalam waktu 24 jam. ABS Mobile memberikan beberapa layanan untama kepada anggota di antaranya adalah layanan keuangan, layanan *Multi Payment,* layanan keagenan, dan layanan *marketplace.*

Di balik pemanfaatan dan pengembangan layanan digital di KSPPS Artha Bahana Syariah yang dilakukan secara masif, pemanfaatan teknologi digital di KSPPS Artha Bahana Syariah juga memiliki risiko yang terkait dengan ancaman *cyber security* terutama pada layanan aplikasi berbasis android dan

internet. Dari hasil wawancara dengan Umini (General Manajer KSPPS Artha Bahana Syariah, 2021) ada beberapa kasus yang pernah terjadi terkait dengan ancaman *cyber security* di antaranya:

Pertama, kasus peretasan dengan modus *Infringements of Privacy* yang dilakukan oleh *cracker* pada Tahun 2019. Kejadian ini berawal ketika IT melakukan update aplikasi ABS Mobile. Update aplikasi ini mengakibatkan aplikasi lama yang telah terinstal di *mobile* anggota menjadi tidak aktif dan harus dilakukan unduh dan instal ulang aplikasi. Setelah instal ulang maka anggota akan mendapatkan nomor notifikasi (OTP) untuk mengaktifkan kembali password ABS Mobile.

Celah dalam proses ini dimanfaatkan oleh *cracker* dengan meminta nomor OTP yang telah dikirimkan oleh sistem kepada anggota mengatasnamakan karyawan KSPPS Artha Bahana Syariah. Sehingga dengan nomor OTP tersebut *cracker* bisa melakukan transaksi dalam rekening anggota melalui mobile lain dengan user dan password yang telah didapatkan. Setelah berhasil mengakses akun anggota maka pelaku melakukan transaksi transfer dana dari rekening anggota ke rekening pelaku.

General manager menyebutkan bahwa kerugian anggota saat itu mencapai 2 juta rupiah dan masalah ini ditangani oleh IT kurang dari dua belas jam. Dalam kasus ini kerugian sejumlah 2 juta masih relatif kecil, dan ini adalah hasil dari kerja keras tim IT karena dapat segera mengatasi *real time* selama 24 jam dengan memblokir seluruh akun anggota dan menutup akses ABS Mobile untuk sementara dan kemudian diperbaiki dan di update kembali dengan segera.

Kasus ini memberikan pelajaran besar untuk KSPPS Artha Bahana Syariah dalam meningkatkan keamanan *cyber*-nya, manajemen mengetahui bahwa ada kebocoran data terutama nomor HP anggota sehingga dimanfaatkan oleh pihak luar, kemudian ABS Mobile yang bisa dibuka di mobile manapun selama seseorang memegang user dan password. Kedua hal ini kemudian dijadikan patokan oleh manajemen untuk melakukan pengamanan data sekaligus meningkatkan kembali sistem keamanan ABS

Mobile *(maintenance)* sehingga tidak terjadi lagi kasus sebagaimana yang telah terjadi.

Kedua, ancaman *cyber security* yang terkait dengan usaha *hacking* yang dilakukan oleh para *hacker* untuk menembus server yang dimiliki oleh KSPPS Artha Bahana Syariah yang di dalamnya menyimpan keseluruhan informasi lengkap data anggota. Dalam segi risiko, ancaman ini akibatnya lebih berbahaya dari kasus yang telah dijelaskan pertama. Ketika server berhasil di *hack* dan dikuasai oleh *hacker* yang tidak bertanggung jawab maka *hacker* bisa melakukan apapun termasuk merusak semua data, menggunakan akun nasabah, atau memindahkan semua dana anggota ke rekening *hacker*. General manajer bersama dengan IT KSPPS Artha Bahana Syariah menjelaskan bahwa terdapat rata-rata lebih dari 100 akun ilegal yang berusaha menerobos sistem keamanan server. Dan tentunya dalam hal ini IT harus selalu berhati-hati dan selalu berupaya meningkatkan keamanan server.

Server dalam hal ini yang digunakan adalah SQL Database Visual Foxpro diperkuat keamanannya dengan VPN *(Virtual Private Network).* VPN merupakan teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri. VPN memiliki beberapa fungsi yang terkait dengan *confidentiality* (kerahasiaan), *data Integrity* (keutuhan data), *origin authentication* (autentikasi sumber), *non-repudiation,* dan kendali akses (Irawan Afrianto & Eko Budi Setiawan).

Virtual private network mengamankan server dari user luar yang ingin menerobos masuk. VPN memberikan ruang transit kepada user-user luar yang tidak memiliki hak akses dalam server KSPPS dan kemudian melakukan block terhadap user tersebut. Dalam jaringan VPN terdapat tembok penghalang untuk user manapun yang berusaha menerobos server, selama user luar tidak mendapatkan izin masuk maka tidak akan bisa

menerobos masuk ke dalam server. istilah tembok penghalang ini dikenal dengan nama *VPN Server Firewall*

Beberapa kasus yang dijelaskan tentu memberikan gambaran bahwa penggunaan teknologi digital berbasis internet memiliki peluang untuk dibobol oleh para pihak yang tidak bertanggung jawab. Apabila pembobolan tersebut berhasil maka akan mengakibatkan kerugian besar pada anggota dan perusahaan. Salah satu konsekuensi yang harus dilakukan oleh KSPPS ketika memanfaatkan dan mengembangkan layanan digital berbasis internet adalah menguatkan manajemen risiko terhadap proses pemanfaatan teknologi digital terutama yang terkait dengan antisipasi ancaman *cyber security.*

2. Penerapan Manajemen Risiko KSPPS Artha Bahana Syariah dalam menghadapi ancaman *Cyber Security*

Ancaman *cyber security* adalah risiko pasti yang timbul akibat dari pemanfaatan teknologi digital dan internet dalam layanan lembaga keuangan. Ancaman ini tidak dapat dijadikan sebagai alasan untuk tidak memanfaatkan teknologi digital dan internet dalam layanan lembaga keuangan. tidak ada pilihan kepada lembaga keuangan untuk menghindari risiko ini dengan cara sama sekali tidak menggunakan teknologi digital dan internet dalam layanannya, karena kalau opsi ini dipilih jelas dalam persaingan bisnis lembaga keuangan tersebut tidak akan mampu bertahan bahkan bisa musnah.

Pilihan satu-satunya untuk lembaga keuangan adalah mengembangkan layanan berbasis digital dan internet serta menerapkan manajemen risiko yang baik untuk menghadapi ancaman *cyber security*. Dengan cara seperti ini maka lembaga jasa keuangan dapat meningkatkan efektifitas dan efisiensi bisnisnya melalui pemanfaatan teknologi digital dan internet sekaligus dapat menangkal ancaman *cyber security* dan melindungi aset anggota dan perusahaan. Sebagaimana yang telah dilakukan di KSPPS Artha Bahana Syariah.

Hasil penelitian ini menunjukkan beberapa pola manajemen risiko yang telah dilakukan oleh KSPPS Artha Bahana Syariah dalam mengantisipasi ancaman *cyber security,* penerapan manajemen risiko di KSPPS Artha Bahana Syariah terkait dengan ancaman *cyber security* minimal dapat diklasifikasikan sebagai berikut:

1. Pengawasan aktif oleh pimpinan

   Penggunaan teknologi informasi KSPPS Artha Bahana Syariah diawasi langsung oleh pimpinan. Dalam hal ini yang berperan adalah General Manager. Pengawasan ini diwujudkan dalam beberapa bentuk di antaranya adalah pimpinan memegang kendali atas akses *database* server yang terhubung ke semua layanan digital, pimpinan langsung mengawal dan mengawasi penyelesaian kasus, dan pengawasan dilakukan secara *full time.* Selain itu pimpinan juga membuat jalur komunikasi *full time* dengan IT agar sewaktu-waktu terjadi masalah terkait dengan pemanfaatan layanan digital dapat diatasi dengan cepat.
2. Kecukupan kebijakan dan prosedur penggunaan Teknologi Informasi.

   Dalam hal kebijakan penggunaan teknologi informasi KSPPS Artha Bahana Syariah sudah memiliki kebijakan yang jelas. Misalnya untuk mengantisipasi kecurangan dan kejahatan yang diakibatkan oleh SDM internal maka KSPPS menetapkan kebijakan hak akses. KSPPS telah membagi hak akses untuk mengantisipasi ancaman *cyber security* yang timbul dari internal perusahaan. Kebijakan hak akses ini di antaranya: 1) vendor pengembang *system core* hanya dapat mengakses server *system core*-nya dan tidak dapat mengakses server ABS mobile ataupun database; 2) vendor pengembang ABS mobile hanya dapat mengakses server yang terkait dengan sistem ABS mobile-nya dan tidak dapat mengakses server *sistem core* ataupun database; 3) IT Internal memiliki akses ke server umum dan memiliki kewenangan untuk memberikan atau menolak hak akses kepada pengembang *sistem core* atau pengembang aplikasi ABS mobile sewaktu akan mengakses server dalam rangka update atau *maintenance*. IT umum tidak memiliki akses

ke server database; dan 4) Akses database hanya dimiliki oleh General Manager. Dan apabila ada keperluan dari IT internal yang mengharuskan melakukan akses ke database maka General Manajer akan memberikan akses (tentunya dalam pengawasan dan pemantauan) serta hanya dapat digunakan untuk sekali akses.

3. Kecukupan proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko teknologi informasi. Manajemen risiko ini dilakukan dalam beberapa kegiatan di antaranya adalah:
   a. Menetapkan dan menerapkan metodologi dan prosedur pengembangan dan pengadaan Teknologi Informasi secara konsisten. Mulai dari desain sistem, percobaan sistem, launching, sampai dengan komitmen untuk *maintenance* sistem dalam rangka meningkatkan keamanan dan pelayanan kepada anggota.
   b. Melakukan uji coba secara memadai dalam pengembangan dan pengadaan suatu sistem hal ini dilakukan untuk memastikan keakuratan dan fungsi sistem sesuai kebutuhan pengguna serta kesesuaian sistem yang satu dengan sistem yang lain. dalam uji coba ini dilakukan penilaian kelayakan sistem, apabila sistem yang diuji coba tidak memenuhi kelayakan maka ada dua kemungkinan, ditolak atau diterima dengan catatan melakukan perbaikan yang dibutuhkan.
   c. Memiliki manajemen perubahan sistem Teknologi Informasi. Perubahan sistem TI ini dibutuhkan mengikuti perkembangan bisnis dan persaingan global. Apabila sebuah sistem sudah usang dan tidak lagi layak untuk digunakan maka manajemen KSPPS berkomitmen untuk memakai sistem yang lebih *support* dalam membantu mengatasi persaingan bisnis.
   d. Memastikan sistem Teknologi Informasi mampu menampilkan kembali informasi secara utuh dengan data yang valid dan dapat dipertanggung jawabkan.

e. Membuat perjanjian tertulis secara yuridis atas perangkat lunak yang dibuat oleh pihak lain (vendor pengembang sistem). Ikatan yuridis ini akan memberikan jaminan kepada KSPPS dari pelanggaran-pelanggaran yang kemungkinan diakibatkan dari kecurangan pihak pengembang.

4. Sistem pengendalian internal atas penggunaan teknologi informasi.

Penerapan manajemen risiko dalam sistem ini di KSPPS Arha Bahana Syariah diwujudkan dalam beberapa hal, yakni :

a. Sistem pengendalian Sumber Daya Manusia IT.

Sistem pengendalian ini diawali dengan proses seleksi yang ketat kepada para calon tenaga IT di awal rekrutmen dan juga pemilihan vendor pengembang sistem yang berasal dari luar perusahaan. Setelah dinyatakan lolos keduanya diikat secara yuridis dan memiliki konsekuensi hukum ketika terjadi penyimpangan atau tindak kejahatan IT.

b. Percobaan sistem

Sebelum dilaunching untuk meningkatkan pelayanan kepada anggota, sistem yang dikembangkan oleh vendor akan diuji coba terlebih dahulu kelayakannya. Ada dua pilihan setelah uji coba yakni ditolak karena tidak sesuai standar dan kriteria, atau diterima dengan catatan perbaikan dan dilanjutkan kontrak.

c. Pengaturan kontrak IT dan Vendor sistem

Perusahaan Membuat kontrak yang berisi komitmen bahwa IT dan vendor sistem harus bersedia datang ke perusahaan untuk melakukan perbaikan ketika terjadi *trouble host.* Selain itu apabila terjadi permasalahan sistem yang terkait dengan ancaman *cyber security* serta kerusakan lain yang sifatnya penting maka IT dan vendor memiliki konsekuensi untuk bekerja secara *real time* 24 jam untuk menyelesaikan masalah tersebut. Konsekuensi ini terbukti dengan hasil penyelesaian peretasan ABS Mobile pada Tahun 2019 yang berhasil diselesaikan dalam waktu kurang dari 12 jam.

d. Pengendalian keamanan fisik dan akses server.

Selain pengendalian internal yang terkait dengan SDM, dalam kaitannya dengan keamanan server perusahaan telah melakukan pengendalian internal. Dalam hal keamanan server secara fisik sehubungan keterbatasan fasilitas dan kemampuan perusahaan dalam mengamankan server secara mandiri maka untuk menghindari kerusakan dan hal lain yang tidak diinginkan server dititipkan kepada penyedia jasa penitipan server yang dipilih oleh perusahaan. Kebijakan penitipan server ini tidak berpengaruh dengan permasalahan akses dan kontrol karena sekalipun server berada di lokasi diluar perusahaan IT masih tetap dapat melakukan akses dengan remot kontrol.

Keamanan akses server perusahaan membuat kebijakan wewenang dan prosedur akses kepada pihak-pihak yang terlibat dalam sistem agar tidak terjadi kecurangan dan kejahatan yang diakibatkan oleh karyawan internal. Hak akses ini telah dijelaskan di kecukupan kebijakan dan prosedur penggunaan teknologi informasi.

Penggunaan VPN *(virtual private network)* dilakukan untuk mengamankan server dari user luar yang ingin menerobos masuk. VPN menghadang user-user luar yang tidak memiliki hak akses dalam server KSPPS dan kemudian melakukan block terhadap user tersebut. Dalam jaringan VPN terdapat *VPN Server Firewall* (tembok penghalang) untuk menghalau user ilegal yang berusaha menerobos server, selama user luar tidak mendapatkan izin masuk maka tidak akan bisa menerobos masuk ke dalam server.

e. Edukasi kepada anggota

Pengendalian internal lainnya yang dilakukan oleh KSPPS adalah edukasi sistem yang selalu dilakukan kepada anggota. Bagaimanapun juga faktor manusia adalah yang paling menentukan untuk keamanan penggunaan teknologi digital dan internet. Peningkatan keamanan siber dilakukan dengan meningkatkan

kesadaran dari pengguna internet (manusia). Manusia menjadi salah satu faktor dalam kesadaran keamanan siber (*cyber security awareness*), dimana manusia seringkali menjadi pertahanan awal dalam pengamanan aset (informasi) (Chen, C. C., dkk., 2008).

Adanya anggota yang cerdas dalam mengamankan akunnya (terdiri dari user, password, nomor OTP, serta identitas lainnya) harus diwujudkan untuk menghindari kerugian yang diakibatkan dari keteledoran dalam penggunaan sistem. Untuk mencapai hal ini maka KSPPS selalu melakukan edukasi, baik edukasi secara langsung yang diberikan di awal ketika anggota bergabung dalam layanan digital, ataupun ketentuan-ketentuan yang telah ada dalam aplikasi digital tersebut.

Penerapan manajemen risiko yang baik dalam penggunaan teknologi informasi terutama dalam pemanfaatan teknologi digital dan internet menjadikan KSPPS Artha Bahana Syariah sukses dalam memanfaatkan perkembangan teknologi untuk efisiensi dan efektifitas bisnisnya. Peningkatan pelayanan kepada anggota dapat dicapai dengan baik dilihat dari banyaknya pengguna ABS Mobile. Kemampuan dalam penyelesaian ancaman *cyber security* dalam waktu singkat, kinerja tim IT yang solid, didukung dengan kebijakan-kebijakan manajemen menjadi salah satu kekuatan yang dimiliki oleh KSPPS Artha Bahana Syariah untuk bersaing dalam bisnis keuangan digital dan meningkatkan layanan kepada para anggotanya. Akan tetapi tentu banyak hal yang perlu dievaluasi terkait dengan segala hal yang telah dilakukan oleh KSPPS Artha Bahana Syariah untuk memperkuat manajemen risiko dalam penggunaan teknologi digital dan internet.

3. Penguatan Manajemen Risiko KSPPS Artha Bahana Syariah dalam Menghadapi Ancaman *Cyber security*

Kebijakan dan strategi untuk menghadapi ancaman *cyber security* di KSPPS Artha Bahana Syariah telah dilakukan dengan baik. Kebijakan dan strategi yang terkait dengan pengembangan dan pengadaan sistem,

operasional TI, jaringan komunikasi, pengamanan informasi, rencana pemulihan bencana, kebijakan tentang penggunaan pihak penyedia jasa telah direncana dan direalisasikan dengan baik. Akan tetapi ada beberapa hal yang perlu dievaluasi dalam rangka penguatan manajemen risiko dalam menghadapi ancaman *cyber security*. Di antara evaluasi dan penguatan manajemen risikonya adalah sebagai berikut:

a. Kebijakan penggunaan IT harus dibakukan dalam bentuk SOP.

   Hasil penelitian yang didapatkan di lapangan ditemukan bahwa kebijakan penggunaan IT yang telah dilakukan dengan baik oleh KSPPS Artha Bahana Syariah diatur langsung oleh General Manager dan belum dibakukan dalam bentuk SOP. Kekurangan ini harus diperhatikan mengingat SOP merupakan satu hal penting yang dapat digunakan sebagai indikator kesuksesan sebuah pekerjaan serta panduan karyawan dalam menyelesaikan pekerjaan dengan baik dan benar.

   Standar Operasional Prosedur (SOP) merupakan pedoman atau acuan untuk melaksanakan tugas dan pekerjaaan sesuai dengan fungsi dari pekerjaan tersebut. Dengan adanya SOP semua kegiatan di suatu perusahaan dapat terancang dengan baik dan dapat berjalan sesuai dengan arah perusahaan serta dapat meminimalisasi kesalahan saat melakukan tugas masing-masing karyawan (Gabriele, 2018). Dalam jangka pendek tanpa SOP mungkin suatu pekerjaan akan baik-baik saja dan bisa diselesaikan sesuai dengan tujuan, akan tetapi untuk kepentingan jangka panjang, SOP memiliki peran penting dalam kesuksesan perusahaan. Adanya SOP bisa digunakan pedoman oleh semua karyawan untuk menyelesaikan pekerjaan, terutama ketika terjadi kasus *turn on* dan *turn off* karyawan.

b. Pengendalian dan pengawasan alur kinerja IT mayoritas berada di tangan General Manager.

   Pengendalian dan pengawasan internal sangat diperlukan untuk kesuksesan KSPPS dalam memanfaatkan teknologi digital dan internet. Akan tetapi ketika semua pengendalian dan pengawasan dilakukan

sendiri oleh General Manager maka hal ini dapat memunculkan risiko baru kaitannya dengan efektifitas kinerja. Diperlukan divisi khusus di atas IT untuk melakukan pengendalian dan pengawasan kinerja IT.

c. Perencanaan jangka panjang membangun penyimpanan server mandiri.
   Server merupakan salah satu komponen penting yang harus dijaga, mengingat dalam server tersimpan semua *database* yang terkait dengan anggota dan perusahaan. Ketika server dititipkan ke penyedia jasa terlebih akses tempat yang jauh maka akan kesulitan ketika terjadi kerusakan. Maka solusi untuk membangun penyimpanan server penting untuk dirumuskan. Penyimpanan server yang dilakukan secara mandiri akan memberikan keleluasaan penuh oleh perusahan untuk melakukan perbaikan *full time* apabila terdapat kerusakan. Apabila langkah ini dipilih tentu memiliki konsekuensi biaya yang tidak sedikit. Maka perencanaan jangka panjang perlu dilakukan untuk mengembangkan tempat penyimpanan server mandiri.
d. Membangun keamanan berlapis dalam transaksi ABS Mobile.
   Keamanan berlapis dalam aplikasi ABS Mobile sangat dibutuhkan untuk menghindari ancaman *cyber security.* Keamanan berlapis dimaksudkan agar akun anggota tidak mudah dibobol oleh pihak-pihak yang tidak bertanggung jawab. Kebutuhan keamanan dalam aplikasi bukan hanya berupa user dan password untuk akses masuk akan tetapi dibutuhkan pin unik atau password khusus untuk otorisasi transaksi. Sehingga apabila user dan password telah dikuasai oleh *cracker* maka anggota masih aman ketika *cracker* tidak mengetahui pin/password untuk otorisasi transaksi.

Beberapa hal yang telah disebutkan merupakan analisis penguatan manajemen risiko yang dapat dilakukan oleh KSPPS Artha Bahana Syariah. Penguatan manajemen risiko ini sangat penting untuk diperhatikan dan ditindaklanjuti agar keamanan *cyber security* dalam pemanfaatan teknologi digital dan internet di KSPPS Artha Bahana Syariah dapat semakin meningkat.

D. Kesimpulan

Penelitian ini menghasilkan kesimpulan bahwa penerapan manajemen risiko di KSPPS Artha Bahana Syariah terkait dengan ancaman *cyber security* dilakukan melalui pengawasan aktif oleh pimpinan, kecukupan kebijakan dan prosedur penggunaan teknologi informasi, kecukupan proses identifikasi, pengukuran, pengendalian, dan pemantauan risiko teknologi informasi, dan sistem pengendalian internal atas penggunaan teknologi informasi. Penguatan manajemen risiko dalam mengantisipasi ancaman *cyber security* diupayakan melalui kebijakan penggunaan IT dengan SOP, pengendalian dan pengawasan alur kinerja IT, perencanaan jangka panjang membangun penyimpanan server mandiri, dan membangun keamanan berlapis dalam transaksi ABS Mobile.

****

Daftar Pustaka

Afrianto, I., & Setiawan, E. B. (2014). Kajian *Virtual Private Network* (Vpn) Sebagai Sistem Pengamanan Data Pada Jaringan Komputer (Studi Kasus Jaringan Komputer Unikom), *Majalah Ilmiah UNIKOM, 12*(1)

Ardiyanti, H. (2014). *Cyber-security* dan tantangan pengembangannya di Indonesia. *Politica, 5*(1)

Arief, B. N. (2001). *Masalah Penegakan Hukum & Kebijakan Penanggulangan Kejahatan*. Bandung: Citra Aditya Bakti.

Arofah, & Priatnasari, (2020). *Internet Banking* dan *Cyber Crime*: Sebuah Studi Kasus di Perbankan Nasional. *Jurnal Pendidikan Akuntansi Indonesia, 18*(2)

Badan Pusat Statistik, Statistik Telekomunikasi Indonesia 2019, https://www.bps.go.id/publication/2020/12/02/be999725b7aeee62d84c6660/statistik-telekomunikasi-indonesia-2019.html. diakses 03/07/2021

Chen, C. C., Medlin, B. D., & Shaw, R. (2008). A Cross-Cultural Investigation of Situational Information Security Awarness Program. *Information Management & Computer Security*. 16(4), 360-376. *doi: 10.1108/09685220810908787.*

Gabriele, (2018). Analisis Penerapan Standar Operasional Prosedur di Departemen Marketing dan HRD PT. Cahaya Indo Persada, *Jurnal AGORA, 6*(1)

https://teknologi.bisnis.com/read/20201110/101/1315765/apjii-1967-juta-warga-indonesia-sudah-melek-internet. dirilis tanggal 10 November 2020, diakses pada tanggal 03/07/2021

https://tekno.kompas.com/read/2021/04/22/14000087/3-keuntungan-bank-digital-untuk-pengguna-?page=all. Dirilis tanggal 24/04/2021. Diakses pada tanggal 03/07/2021

https://www.cnbcindonesia.com/tech/20200907140920-37-184917/waspadalah-ini-kasus-pembobolan-m-banking-yang-terjadi-di-ri. dirilis pada tanggal 07 September 2020, dan diakses pada tanggal 03 Juli 2021

https://www.cnnindonesia.com/nasional/20190809201016-12-419999/polisi-ringkus-tersangka-pembobol-kartu-kredit-sebesar-rp1-m. dirilis pada tanggal Jumat, 09/08/2019 dan diakses pada tanggal 03 Juli 2021

Jannah, I. F., Dkk. (2020). Pengaruh Kualitas Digital Banking Terhadap kepuasan Nasabah. *JIHBIZ; Global Journal of Islamic Banking and Finance,* 2(1)

Moleong, L. J. (2008). *Metodologi Penelitian Kualitatif; Edisi Revisi*. Bandung: PT. Remaja Rosdakarya

Mawarni, R., dkk. (2021). Penerapan Digital Banking Bank Syariah Sebagai Upaya Customer Retention Pada Masa Covid-19. *AL-IQTISHOD: Jurnal Pemikiran dan Penelitian Ekonomi Islam, 9*(2)

Peraturan Otoritas Jasa Keuangan No. 1/POJK.5/2015 Tentang Penerapan Manajemen Risiko Lembaga Keuangan Non Bank

Pratama, P. A. E., & Pratika, M. T. S. (2020). Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000: 2018. *Jurnal Telematika institut Teknologi Harapan Bangsa Bandung, 15*(2)

Radu, R. (2014) Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace dalam Jan Frederik Kremer & Benedikt Muller (ed), *Cyberspace and International Relations: Theory, Prospect and Challenges*. Bonn: Springer.

Raharjo, A. (2002). *Cybercrime, Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: Citra Aditya Bahkti

Respati, H. (2008). Teknologi Informasi Bank Pada Era *Cyberbanking*. *Jurnal Ekonomi Modernisasi, 4*(3)

Sugiyono. (2009). *Metode Penelitian Bisnis*. Bandung: Alfabeta

Sulisrudatin. (2018). Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara, 9*(1)

Susilawati, L., & Nicola. (2020). Pengaruh Layanan Perbankan Digital pada Kepuasan Nasabah Perbankan, *JMM, Jurnal Manajemen Maranatha, 19*(2)

Wawancara, Umini (General Manajer KSPPS Artha Bahana Syariah) pada tanggal 9 September 2021 jam 13.00 s.d 15.30 di Kantor Pusat KSPPS Artha Bahana Syariah.

www.arthabahana.com

Zulganef. (2008). *Metode Penelitian Sosial dan Bisnis*. Yogyakarta: Graha Ilmu