# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

PT BFI Finance Indonesia Tbk (BFI Finance) didirikan pada tahun 1982 dengan nama PT Manufacturers Hanover Leasing Indonesia. BFI Finance sendiri pada awalnya merupakan perusahaan patungan antara Manufacturers Hanover Leasing Corporation dari Amerika Serikat dan pemegang saham lokal. Dalam perkembangannya BFI Finance adalah perusahaan pembiayaan yang telah lama berdiri di Indonesia dan menjadi perusahaan pembiayaan pertama yang mencatatkan sahamnya di Bursa Efek Jakarta dan Bursa Efek Surabaya (sekarang Bursa Efek Indonesia atau BEI). BFI Finance juga termasuk perusahaan pembiayaan besar di Indonesia, dengan jaringan dan cakupan produk terluas, didukung oleh 11.207 karyawan di 271 outlet yang tersebar di 35 provinsi. Sejak 2013, kantor pusat Perusahaan berlokasi di BFI Tower, Sunburst CBD Lot 1.2, Jl. Kapt. Soebijanto Djojohadikusumo, BSD City, Tangerang Selatan 15322, Provinsi Banten.

Salah satu komitmen perusahaan adalah untuk melakukan transformasi digital yang menyeluruh dengan tujuan tetap menjadi pemimpin dalam industri pembiayaan. Meningkatkan layanan pelanggan adalah tujuan utama transformasi digital BFI Finance. Proses bisnis yang sepenuhnya terdigitalisasi akan menguntungkan perusahaan dan pelanggan. Sejak akhir 2021, BFI Finance telah memulai beberapa proyek percontohan, yang akan terus dikembangkan hingga akhir 2022. Perusahaan akan secara bertahap mengubah model bisnisnya dari yang bergantung pada proses manual ke model yang sepenuhnya terdigitalisasi melalui proyek-proyek ini.

Tujuan lain dari transformasi digital yang dilakukan adalah untuk bisa responsif terhadap perubahan kebutuhan pelanggan yang terus berubah seiring dengan kemajuan teknologi. Berdasarkan laporan tahunan BFI Finance tahun 2022, setiap langkah dalam proses transformasi digital dilakukan dengan hati-hati, baik dalam hal alur kerja maupun dalam skalanya. Dengan metode kerja ini sangat penting untuk memastikan bahwa inovasi yang terkait dengan transformasi digital

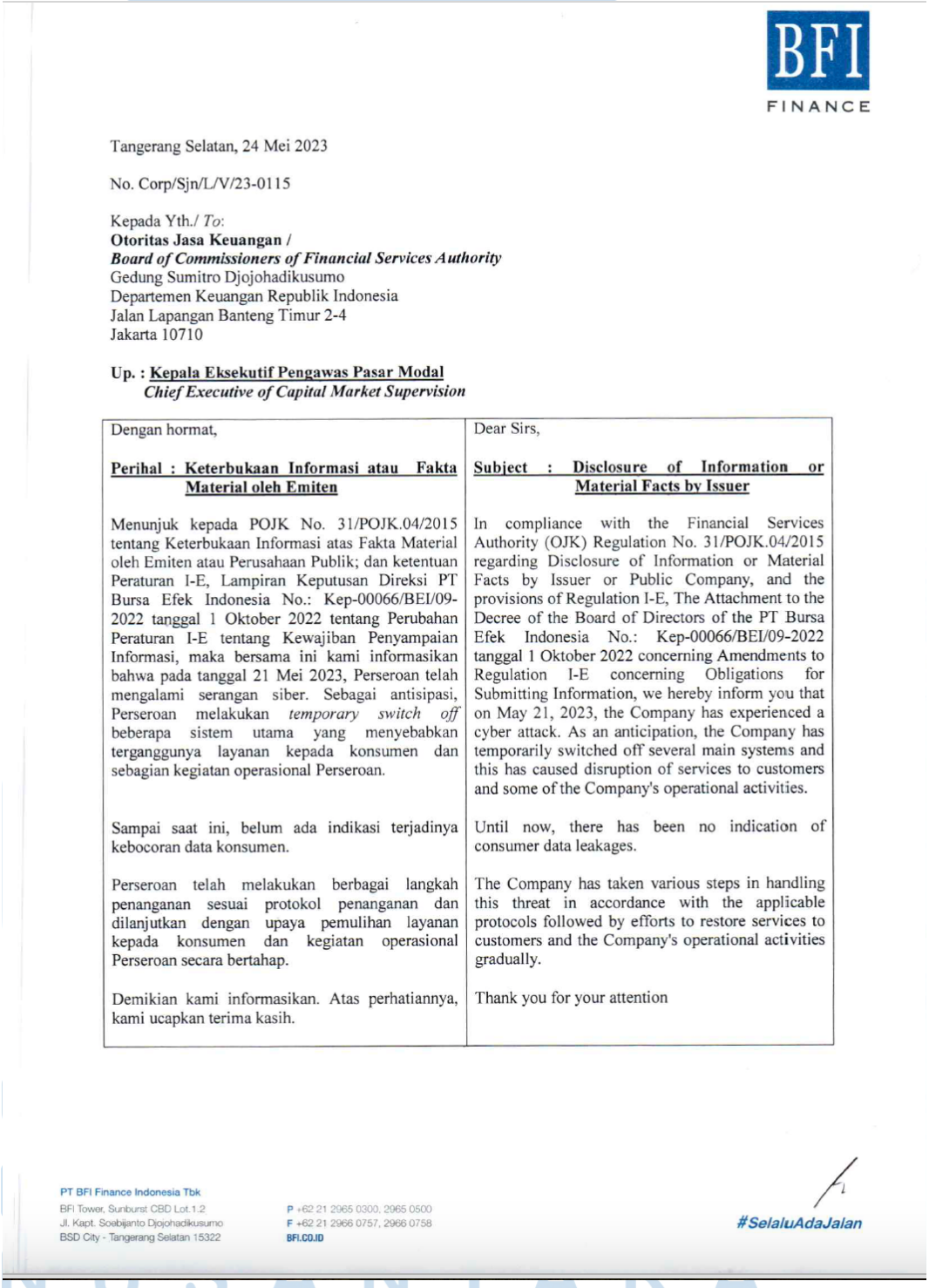
memiliki efek yang diinginkan tanpa menimbulkan bahaya baru yang tidak dapat diprediksi.

Untuk mencapai tujuan tersebut, departemen Teknologi Informasi (TI) BFI Finance telah memulai pengembangan strategi TI pada tahun 2022. Fokus utamanya adalah menciptakan aplikasi dan sistem baru untuk meningkatkan dan memodernisasi sistem yang saat ini digunakan. Upaya ini dilakukan untuk memastikan bahwa berbagai infrastruktur TI dan modul dapat memberikan manfaat terbaik bagi pengguna internal dan semua orang yang terlibat dalam bisnis BFI Finance. Tentu saja, inisiatif ini akan menjadi tantangan yang tidak mudah bagi departemen TI yang saat ini berjumlah 284 orang. Tidak hanya aplikasi dan sistem yang baru, transformasi digital di bidang infrastruktur pun perlu dilakukan. Bahkan sejak tahun 2020 BFI Finance sudah mengadopsi teknologi *Cloud Computing*. Dari sisi jaringan komunikasi, cabang-cabang yang tersebar di seluruh Indonesia sudah terkoneksi dengan kantor pusat melalui jaringan *private* yang memiliki standar keamanan internasional.

Upaya transformasi digital yang sedang berlangsung di tahun 2022 juga disertai dengan upaya yang berkelanjutan untuk memperkuat keamanan informasi. Untuk mengurangi risiko yang terkait dengan keamanan informasi, perhatian khusus diberikan pada perlindungan data konsumen serta integritas komponen TI lainnya. Di tengah transformasi menjadi lembaga pembiayaan yang adaptif dan mampu menyediakan solusi yang sesuai dengan era digital, poin keamanan menjadi strategi penting bagi bisnis untuk mempertahankan kepercayaan pelanggan. Pada tanggal 30 Oktober 2023, BFI Finance mendapatkan sertifikasi ISO IEC 27001:2013 dalam bidang Sistem Manajemen Keamanan Informasi (SMKI) oleh BSI Group Indonesia.

Transformasi digital juga tidak terlepas dari beberapa tantangan, salah satunya adalah tantangan keamanan. Serangan siber merupakan risiko terbesar yang harus dihadapi oleh para industri keuangan salah satu contohnya adalah PT BFI Finance, seperti yang terjadi pada tahun 2023 ketika BFI Finance mengalami serangan siber yang mengganggu layanan mereka. Menurut Li & Liu (2021) serangan siber adalah serangan yang melibatkan penggunaan berbagai kemampuan,

seperti perang elektronik, psikologis, jaringan komputer, tipuan militer, dan keamanan. Serangan ini bertujuan untuk memengaruhi keputusan manusia di lembaga-lembaga nasional (Hart et al., 2020).



BFI FINANCE

Tangerang Selatan, 24 Mei 2023

No. Corp/Sjn/L/V/23-0115

Kepada Yth./ *To*:
**Otoritas Jasa Keuangan /**
***Board of Commissioners of Financial Services Authority***
Gedung Sumitro Djojohadikusumo
Departemen Keuangan Republik Indonesia
Jalan Lapangan Banteng Timur 2-4
Jakarta 10710

**Up. : Kepala Eksekutif Pengawas Pasar Modal**
***Chief Executive of Capital Market Supervision***

| | |
|---|---|
| Dengan hormat, | Dear Sirs, |
| **Perihal : Keterbukaan Informasi atau Fakta Material oleh Emiten** | **Subject : Disclosure of Information or Material Facts by Issuer** |
| Menunjuk kepada POJK No. 31/POJK.04/2015 tentang Keterbukaan Informasi atas Fakta Material oleh Emiten atau Perusahaan Publik; dan ketentuan Peraturan I-E, Lampiran Keputusan Direksi PT Bursa Efek Indonesia No.: Kep-00066/BEI/09-2022 tanggal 1 Oktober 2022 tentang Perubahan Peraturan I-E tentang Kewajiban Penyampaian Informasi, maka bersama ini kami informasikan bahwa pada tanggal 21 Mei 2023, Perseroan telah mengalami serangan siber. Sebagai antisipasi, Perseroan melakukan *temporary switch off* beberapa sistem utama yang menyebabkan terganggunya layanan kepada konsumen dan sebagian kegiatan operasional Perseroan. | In compliance with the Financial Services Authority (OJK) Regulation No. 31/POJK.04/2015 regarding Disclosure of Information or Material Facts by Issuer or Public Company, and the provisions of Regulation I-E, The Attachment to the Decree of the Board of Directors of the PT Bursa Efek Indonesia No.: Kep-00066/BEI/09-2022 tanggal 1 Oktober 2022 concerning Amendments to Regulation I-E concerning Obligations for Submitting Information, we hereby inform you that on May 21, 2023, the Company has experienced a cyber attack. As an anticipation, the Company has temporarily switched off several main systems and this has caused disruption of services to customers and some of the Company's operational activities. |
| Sampai saat ini, belum ada indikasi terjadinya kebocoran data konsumen. | Until now, there has been no indication of consumer data leakages. |
| Perseroan telah melakukan berbagai langkah penanganan sesuai protokol penanganan dan dilanjutkan dengan upaya pemulihan layanan kepada konsumen dan kegiatan operasional Perseroan secara bertahap. | The Company has taken various steps in handling this threat in accordance with the applicable protocols followed by efforts to restore services to customers and the Company's operational activities gradually. |
| Demikian kami informasikan. Atas perhatiannya, kami ucapkan terima kasih. | Thank you for your attention |

PT BFI Finance Indonesia Tbk
BFI Tower, Sunburst CBD Lot.1.2
Jl. Kapt. Soebijanto Djojohadikusumo
BSD City - Tangerang Selatan 15322

P +62 21 2965 0300, 2965 0500
F +62 21 2966 0757, 2966 0758
BFI.CO.ID

#SelaluAdaJalan

Hormat kami, / *Regards*,
**PT BFI Finance Indonesia Tbk.**

**Sudjono**
Direktur/*Director*

Tembusan Yth.:
1. Kepala Eksekutif Pengawas IKNB / Chief Executive of Non Bank Financial Industry Supervision
2. Direksi PT Bursa Efek Indonesia / Board of Director PT Bursa Efek Indonesia

*Gambar 1-1 Konferensi Pers PT BFI Finance Terkait Serangan Siber*

Sumber: Keterbukaan Informasi - www.bfi.co.id (2023)

Sesuai dengan Peraturan Nomor Kep-00066/BEI/09-2022 dan juga Peraturan Otoritas Jasa Keuangan (OJK) Nomor 31/POJK.04/2015, PT BFI

Finance mengadakan press release mengenai serangan siber pada tanggal 24 Mei 2023. Informasi mengenai serangan siber disampaikan dalam rangka keterbukaan dan kepatuhan BFI Finance terhadap aturan dan regulasi yang mengatur kewajiban perusahaan dalam memberikan informasi yang relevan dan penting kepada publik serta lembaga terkait. Ini mencerminkan komitmen BFI Finance dalam mematuhi aturan dan memberikan keterbukaan kepada publik mengenai peristiwa yang dianggap material dan penting, seperti serangan siber yang BFI alami.

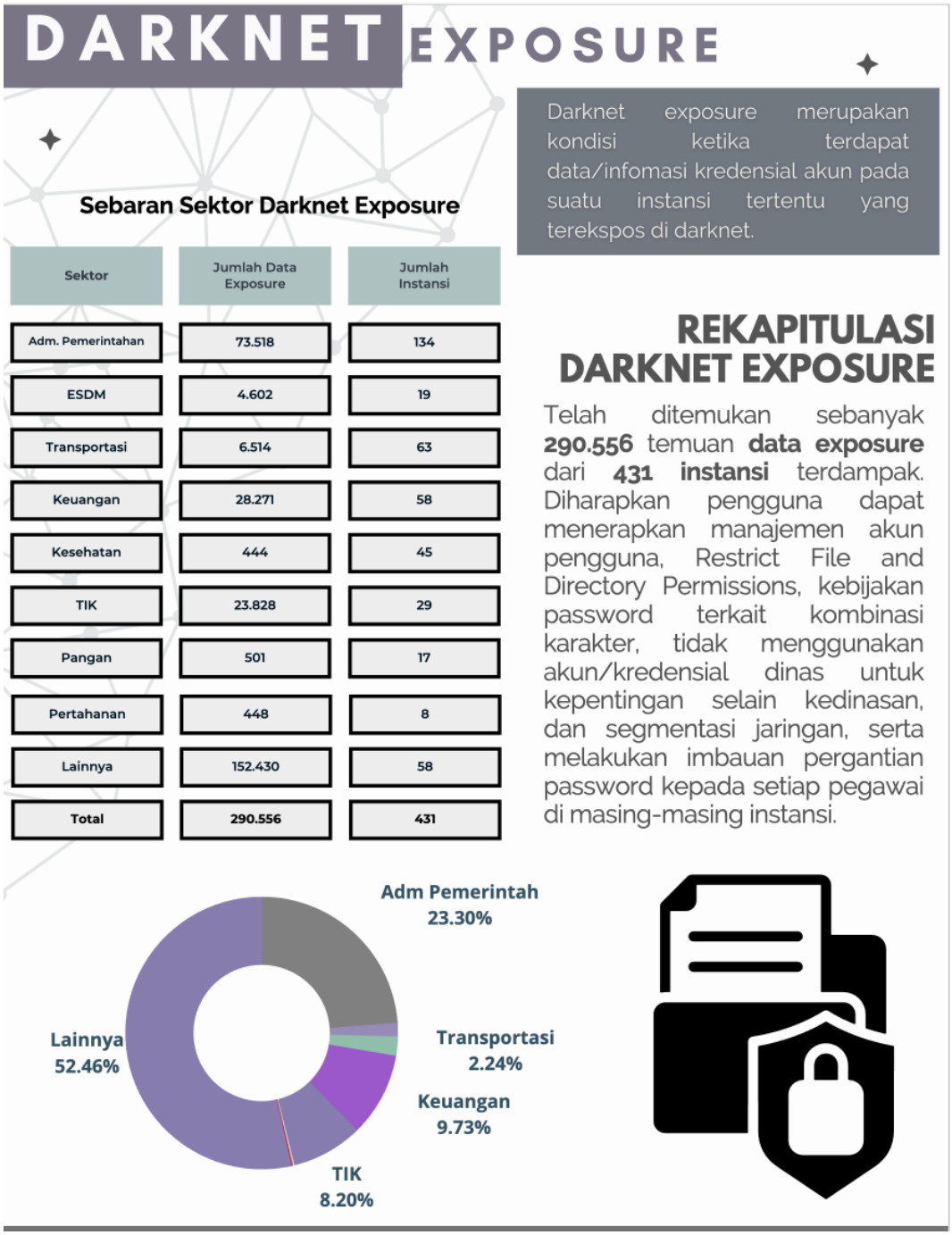
Laporan tahunan 2023 mengemukakan bahwa Inisiatif TI di tahun 2023 difokuskan pada peremajaan sistem originasi dan penguatan keamanan TI secara menyeluruh, terutama aspek pencegahan, pemantauan, dan kesadaran karyawan. Sejak tahun 2020, PT BFI Finance telah menyelenggarakan pelatihan terkait kepada karyawan untuk meningkatkan kesadaran keamanan data-data penting dari berbagai fungsi bisnis. Disamping hal itu, BFI Finance juga melakukan peninjauan terhadap setiap aspek yang berpotensi memengaruhi bisnisnya dan akan memperkuat sistem manajemen risiko terkait dengan transformasi digital.

BFI Finance telah mengambil langkah preventif pasca serangan siber untuk mengurangi risiko kebocoran data nasabah. Salah satunya adalah menggunakan konsultan keamanan siber dan ini mencerminkan betapa pentingnya perlindungan data dalam era transformasi digital. Salah satu langkah penting yang mulai dilakukan adalah pengamanan aset TI (Teknologi Informasi).

BFI Finance saat ini memiliki lebih dari 9.000 perangkat digital mulai dari PC, laptop, server dengan jumlah pengguna kurang lebih 11.000 yang tersebar di lebih dari 200 kantor cabang. Adapun keterbatasannya dari keseluruhan tim TI yang benar-benar terlibat langsung dengan asset digital, kurang lebih hanya 30 orang. Faktor ini tidak sebanding dengan jumlah aset TI yang dimiliki dan dampaknya untuk melakukan pemantauan aset, *software patching* membutuhkan waktu yang cukup lama. Efek yang ditimbulkan ketika terjadi serangan siber adalah membutuhkan waktu yang cukup lama bahkan bisa sangat terlambat untuk menanggulanginya. Tentu kondisi ini tidak diharapkan oleh perusahaan, seharusnya ketika terjadi serangan aset-aset yang masuk ke dalam list *critical* atau penting seperti server dan perangkat penting lainnya itu sudah teridentifikasi dan

terlindungi dengan baik. Peran *Asset Management* diperlukan untuk klasifikasi aset TI (Teknologi Informasi) berdasarkan sensitivitas dan nilai bisnisnya. Klasifikasi ini membantu dalam memprioritaskan upaya keamanan siber berdasarkan konsep dari *Framework NIST* dan juga penentuan level kontrol akses yang diperlukan berdasarkan konsep *Framework PPT*. Aset yang lebih sensitif akan memerlukan perlindungan dan kontrol yang lebih ketat.

Berbicara mengenai IT *Asset Management* faktor teknologi berperan penting disini, karena dibutuhkan pendataan, pemantauan dan mitigasi resiko dengan menggunakan alat yang canggih. Tanpa mengetahui aset yang dimiliki, sulit untuk mengidentifikasi risiko keamanan siber dan menetapkan peran dan kontrol akses yang tepat. Informasi yang dikumpulkan melalui IT *Asset Management*, seperti masa pakai aset dan riwayat perawatan, dapat digunakan untuk membuat keputusan keamanan yang lebih baik. Misalnya, mengetahui aset mana yang mendekati akhir masa pakainya dapat membantu menentukan apakah lebih baik meningkatkan keamanannya atau menggantinya.




*Gambar 1-2 Laporan Mengenai Kebocoran Data Agustus 2023*

Sumber: Badan Siber Dan Sandi Negara (BSSN) (2023)

Berbicara mengenai kebocoran data, laporan dari BSSN (Badan Siber dan Sandi Negara) bulan Agustus tahun 2023 menyebutkan ada sekitar 28.271 data dari 29 lembaga atau instansi keuangan di Indonesia yang tersebar di *Darknet*. Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, dan Guttorm Sindre (2020) menyatakan

*Darknet*, yang secara umum terkait dengan jaringan tersembunyi di Internet, awalnya dibuat oleh Laboratorium Penelitian Angkatan Laut Amerika Serikat untuk komunikasi anonim. Kumpulan situs web di *darknet* sering disebut sebagai *darkweb*, bagian tersembunyi dari internet yang tidak terindeks dan tidak dapat dijangkau melalui mesin pencari biasa. Meskipun sebagian besar isi dari web tersembunyi tersebut adalah legal, *darkweb* sering berisi konten yang terkait dengan kegiatan kriminal. Sebuah studi oleh Moore dan Rid (2016) memperkirakan sekitar 57% situs web TOR memfasilitasi kegiatan kriminal seperti perdagangan narkoba, senjata, pembunuhan, dan pornografi anak. *Darknet* juga merupakan topik yang kerap menjadi sorotan dalam bidang keamanan siber. Meskipun bagi sebagian orang, jaringan tersembunyi di Internet digunakan untuk kebebasan, bagi yang lain, *darknet* dianggap sebagai tempat bagi kegiatan kriminal. Media sering menggambarkan *Darknet* sebagai lingkungan di mana kegiatan ilegal tumbuh subur, yang menimbulkan kekhawatiran baik dari masyarakat maupun pemerintah (Mirea, Wang, & Jung, 2019).

**1.2.Rumusan Masalah**

Era transformasi digital menuntut perlindungan data yang lebih efektif dan mengurangi risiko terhadap potensi serangan siber di masa mendatang. Pada tanggal 21 Mei 2023, BFI Finance mengalami serangan siber yang mempengaruhi sejumlah sistem utama perusahaan. Serangan tersebut menyebabkan dampak langsung pada layanan yang diberikan kepada konsumen dan sebagian kegiatan operasional perusahaan.

Ketika melakukan proses pemulihan ada berbagai masalah yang dihadapi terutama di bagian aset TI. Menurut Stone et al., (2018) dalam laporannya mengenai *asset management* di NIST SP 1800-5 rata-rata perusahaan mengalami salah satu atau beberapa masalah aset TI seperti kurangnya visibilitas aset TI, kontrol konfigurasi yang tidak efektif, manajemen *patch* yang tidak konsisten, kurangnya manajemen *vulnerability* perangkat lunak, tidak adanya gambaran terpadu tentang aset TI perusahaan, dan kurangnya repositori terpusat untuk aset TI.

Belajar dari kasus tersebut, bagaimana BFI Finance dapat meningkatkan keamanan sibernya, terutama dalam hal mengenai IT *asset management* yang dapat diandalkan?

### 1.3.Tujuan Transformasi Digital

Ada banyak ancaman keamanan siber yang mengintai di era transformasi digital termasuk serangan *ransomware*, pencurian data, serta kebocoran informasi sensitif pengguna dan perusahaan. Masalah ini harus menjadi fokus utama dalam transformasi digital, yang memerlukan solusi terukur dan efektif untuk melindungi informasi rahasia dan kelangsungan operasional perusahaan di tengah ancaman siber yang semakin berkembang. *Cybersecurity* atau keamanan siber, menurut ISO/IEC 27032:2012, adalah upaya untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi dalam lingkungan yang kompleks. Lingkungan ini muncul dari interaksi antara manusia, perangkat lunak, dan layanan di internet menggunakan perangkat teknologi dan jaringan yang terhubung. Saat ini, *cybersecurity* dianggap sebagai salah satu komponen kritis dalam manajemen risiko perusahaan, karena jumlah pelanggaran siber yang terus meningkat menyebabkan berbagai biaya kritis bagi organisasi dan individu (Lee, 2021)

Tujuan penelitian ini adalah meningkatkan keamanan siber perusahaan terhadap aset TI (Teknologi Informasi) di tengah ancaman serangan siber supaya BFI Finance dapat melakukan transformasi digital secara efektif dan efisien. Stone et al., (2018) dalam laporan NIST SP 1800-5, mengemukakan bahwa solusi manajemen aset teknologi informasi (ITAM) yang efektif harus memiliki beberapa karakteristik penting. Solusi ITAM yang baik dapat menghubungkan aset fisik dan virtual serta memberikan manajemen gambaran lengkap tentang apa, di mana, dan bagaimana aset digunakan. ITAM meningkatkan visibilitas bagi analis keamanan, yang mengarah pada pemanfaatan aset dan keamanan yang lebih baik. Berdasarkan NIST.SP.1800-5, implementasi IT Asset Management mencakup beberapa aspek dari kemampuan keamanan IT seperti:

1. **Comprehensive Risk Assessment & Management**: - IT Asset Management membantu dalam mengidentifikasi dan mengelola risiko yang terkait dengan aset IT. Dengan mengetahui lokasi, konfigurasi, dan status

aset, organisasi dapat melakukan penilaian risiko yang lebih akurat dan mengimplementasikan langkah-langkah mitigasi yang tepat.

2. **Incident Response & Recovery:** - IT Asset Management memberikan visibilitas yang diperlukan untuk merespons insiden keamanan dengan cepat dan efektif. Dengan mengetahui aset mana yang terpengaruh oleh insiden, tim respons dapat mengambil tindakan yang tepat untuk memulihkan operasi dan mengurangi dampak insiden.
3. **Continuous Improvement**: - Implementasi IT Asset Management memungkinkan organisasi untuk terus memantau dan meningkatkan pengelolaan aset. Dengan data yang akurat dan terkini tentang aset, organisasi dapat melakukan identifikasi perbaikan dan melakukan perubahan yang diperlukan untuk meningkatkan efisiensi dan keamanan.

Beberapa karakteristik penting dari solusi ITAM yang efektif meliputi integrasi dengan sistem manajemen aset, keamanan, dan jaringan yang ada, di mana solusi ITAM harus dapat berkomunikasi dengan perangkat dan sistem keamanan lainnya seperti *firewall*, IDS (Intrusion Detection System), dan *Identity Access & Management System*. Komunikasi dengan perangkat dan sistem keamanan lainnya dilakukan melalui API (Application Programming Interface). Tidak lupa diperlukan pemantauan yang baik terhadap aset untuk memungkinkan pemantauan yang efektif dalam mendeteksi anomali atau penyalahgunaan. Terakhir ada faktor manajemen risiko yang membantu dalam mengidentifikasi dan mengurangi risiko yang terkait dengan aset.

## 1.4.Manfaat Proyek

### 1.4.1. Manfaat Akademis

- Pengembangan *Framework*, model *Framework* menggunakan NIST *Cybersecurity Framework* dan *Profile for Ransomware Risk Management* sebagai acuan untuk menentukan dimensi, variabel, dan tingkat kematangan *cybersecurity* organisasi. *Framework* NIST tersebut akan digabungkan dengan *Framework* dari *PPT (People, Process & Technology)*.
- Analisa *Framework* dengan maturity model NIST akan digunakan untuk mengukur, memprioritaskan dan meningkatkan kematangan *cybersecurity*

organisasi, khususnya dalam aset TI untuk menghadapi risiko ransomware. Sedangkan Analisa *Framework* dengan maturity model *PPT (People, Process & Technology)* akan digunakan sebagai strategi untuk melengkapi maturity model NIST dari perspektif *control*.

- Melakukan validasi dan verifikasi model maturity model melalui survei, wawancara, observasi, atau dokumen, dan menganalisisnya dengan menggunakan metode statistik, kualitatif, atau campuran. Hasil analisa berupa rekomendasi untuk perbaikan dan pengembangan lebih lanjut.

### 1.4.2. Manfaat Operational dan Fungsional:

- Mampu memetakan dan melakukan alignment antara permasalahan *IT Asset Management* dan *cybersecurity* akibat *ransomware* yang dihadapi oleh PT BFI Finance. Melalui pengukuran yang dilakukan oleh NIST *Cybersecurity Framework* dan *Profile for Ransomware Risk Management* serta PPT *(People, Process & Technology)* diharapkan dapat membantu pada peningkatan sumber daya manusia dan koordinasi (People), verifikasi efektivitas proses dan kebijakan (Process), serta otomatisasi dan continous improvement (Technology) sehingga perusahaan dapat menjadi lebih resilien, berdaya saing, dan kontributif di era digital.
- Melakukan identifikasi gap dan hambatan yang menghambat transformasi digital *Cybersecurity* terutama di bagian aset TI serta peluang dan tantangan yang dapat dimanfaatkan dan diatasi oleh perusahaan.
- Ada pengembangan *cost-benefit/TCO (Total Cost Of Ownership) /Total Economic Impact* dari peningkatan teknologi *cybersecurity* dan IT *Asset Management* yang digunakan atau direncanakan oleh PT BFI Finance.

### 1.4.3. Manfaat untuk Peneliti:

- Mendapatkan peningkatan pengetahuan, keterampilan, dan soft skill yang diperoleh dari proses penelitian melalui konsep-konsep dan teori-teori terkait seperti IT *Asset Management*, NIST *Cybersecurity Framework*, PPT *(People, Process & Technology) Framework* dan *maturity model*.