BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dampak yang dirasakan oleh PT BFI Finance pasca-*cyberattack* sangat mempengaruhi bisnis dan kegiatan operasional. Langkah pengamanan apa yang harus dilakukan dan bagaimana cara melakukannya adalah salah satu pertanyaan yang mungkin timbul.

Berawal dari sana, maka penelitian mengenai digital transformasi ini dilakukan. Penelitian dilakukan dengan mengkombinasikan dua *Framework* yaitu *Framework* PPT dan NIST dan berdasarkan hasil analisa terlihat bahwa dalam rangka memperkuat keamanan siber pasca-*cyberattack*, ada prioritas yang harus diberikan pada dimensi *Identify*, khususnya pada manajemen aset TI. Dimensi *identify* ini merupakan fondasi yang akan menentukan efektivitas dari semua langkah keamanan lainnya. Tidak lupa juga hasil pengukuran dari DMM PPT (People, Process dan Technology) juga membantu melengkapi akan peningkatan kesadaran akan risiko keamanan siber.

Optimisasi proyek manajemen aset diharapkan akan membawa PT BFI Finance menuju tingkat kematangan yang lebih tinggi. Estimasi perkiraan biaya dari proyek ini akan kembali dalam waktu 5 tahun. Adapun ada perkiraan penghematan sebesar 883 juta rupiah setiap tahunnya. Proyek transformasi digital ini memiliki risiko yang menengah namun memberikan efek yang penting terhadap keamanan perusahaan.

Integrasi hasil *Framework* PPT dan NIST ke dalam proyek manajemen aset juga diharapkan dapat membantu pada peningkatan sumber daya manusia dan koordinasi (*People),* verifikasi efektivitas proses dan kebijakan (*Process*), serta otomatisasi dan *continous improvement* (*Technology*). Pada akhirnya semua *Framework* akan bersinergi menciptakan fondasi yang kuat untuk keamanan siber yang tangguh.

Dengan demikian, proyek manajemen aset yang efektif dalam *Identify* disertai dengan integrasi aspek *People, Process dan Technology* menjadi kunci utama untuk memastikan keamanan siber yang komprehensif di PT BFI Finance.

5.2 Saran

Berdasarkan dari hasil penelitian dan pengukuran pasca insiden, PT BFI Finance Indonesia diharapkan untuk dapat menuju ke tingkat yang lebih dari yang ada sekarang. Dalam perjalanannya, pendekatan *Framework* NIST dan PPT dapat memberikan dampak yang signifikan terhadap peningkatan *cybersecurity* dan IT *asset management* perusahaan. Hasil integrasi kedua f*ramework* ini membantu memperkuat dimensi *Identify,* yang mana merupakan fondasi penting dalam manajemen keamanan siber. Kedua *framework* juga dapat membantu memprioritaskan upaya keamanan siber sesuai konsep dari *Framework NIST* dan juga penentuan level kontrol akses yang diperlukan sesuai dengan konsep *Framework PPT*. Aset yang lebih sensitif akan memerlukan perlindungan dan kontrol yang lebih ketat. Selain itu, pengukuran dari DMM PPT (People, Process, dan Technology) membantu meningkatkan kesadaran akan risiko keamanan siber, yang penting untuk menciptakan budaya keamanan yang kuat dalam organisasi.

Menurut hasil penelitian, dari segi investasi proyek peningkatan *cybersecurity* dan IT *asset management* yang mengadopsi kerangka kerja NIST dan PPT ini masih layak untuk diimplementasika. Berdasarkan estimasi, proyek ini diharapkan akan memberikan penghematan sebesar 883 juta rupiah setiap tahunnya, dengan perkiraan biaya yang akan kembali dalam waktu 5 tahun. Selain itu, investasi dalam keamanan siber tidak hanya melindungi nilai tetapi juga dapat menciptakan nilai dengan meningkatkan efisiensi operasional dan mengurangi risiko kerugian akibat insiden siber. Oleh karena itu, dari segi investasi, proyek ini dapat dianggap layak dan memberikan manfaat jangka panjang bagi perusahaan.

Dalam konteks manajemen proyek, risiko yang terkait dengan proyek peningkatan cybersecurity dan IT asset management yang mengadopsi kerangka kerja NIST dan PPT masih dapat diterima. Meskipun proyek ini memiliki risiko yang menengah, langkah-langkah mitigasi risiko yang tepat dapat diimplementasikan untuk mengurangi dampak negatifnya. Risiko-risiko tersebut

termasuk peningkatan koordinasi dan staf, verifikasi keamanan, percepatan waktu respon, dan peningkatan otomatisasi dalam kontrol teknologi. Dengan pendekatan yang sistematis dan terstruktur, risiko-risiko ini dapat dikelola dengan baik, sehingga proyek ini tetap dapat memberikan manfaat yang signifikan bagi keamanan siber perusahaan.

5.3 Saran Untuk Penelitian Selanjutnya

Adapun saran – saran bagi peneliti selanjutnya adalah sebagai berikut:

1. Penelitian ini banyak mengambil sampel dari departement teknologi. Untuk penelitian selanjutnya, pengambilan sampel data yang digunakan bisa lebih luas.
2. Bagi penelitian selanjutnya, variabel kuesioner atau subkategori bisa diperluas untuk menambah varian data yang dihasilkan.
3. Penelitian ini dilakukan dengan waktu yang terbatas, untuk mencapai tingkat yang diharapkan perlu penelitian lebih lanjut supaya lebih akurat.
4. Penelitian selanjutnya agar mempertimbangkan penerapan Standar Internasional Keamanan ISO 27001. Standar ini mencakup aspek Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi, yang telah diadopsi oleh BSSN (Badan Siber dan Sandi Nasional) dan telah menjadi beberapa Standar Nasional Indonesia terkait keamanan siber dan sandi. Dengan penerapan standar ini dapat menjadi acuan penting bagi perbaikan penelitian ini ataupun untuk BFI Finance.