BAB I
PENDAHULUAN

1.1 Latar Belakang

Umumnya suatu perusahaan atau organisasi menggunakan teknologi informasi untuk mendukung keberlanjutan sistem informasi yang sedang berjalan. berdasarkan beberapa para ahli teknologi informasi dapat dimanfaatkan untuk berbagai kebutuhan bisnis, manfaat yang didapatkan dari hal tersebut diantaranya: penghematan dan ketepatan waktu, meningkatkan produktivitas, dan akurasi informasi yang lebih terjamin [1]. Sistem informasi dalam suatu organisasi dapat dipandang sebagai suatu sistem yang menyediakan informasi kepada seluruh tingkatan organisasi sesuai kebutuhan. Sistem ini menyimpan, mengambil, memodifikasi, memproses, dan mengkomunikasikan informasi yang diterima dari sistem informasi atau perangkat sistem lainnya. Sistem informasi adalah suatu kerangka kerja yang mengkoordinasikan sumber daya manusia dan komputer untuk mengubah masukan menjadi keluaran (informasi) untuk mencapai tujuan organisasi[2]. Walaupun tidak semua teknologi informasi dalam mengelola sistem informasi berjalan sesuai dengan yang dinginkan, salah satunya ialah keamanan data.

Apabila perusahaan tidak mengoptimalkan keamanan data yang ada di perusahaan, maka kesempatan untuk diserang akan tinggi dan akan ada berbagai ancaman yang masuk dan menyerang *system.* Ada berbagai macam ancaman *cybersecurity seperti, DoS (Denial of Service), Malware, Phising, Credential Reuse, SQL Injection, Cross Site Scripting (XSS)* dan *Man in the Middle.* Serangan-serangan tersebut bertujuan untuk mendapatkan keuntungan dengan berbagi cara dan dalam penggunaannya akan timbul berbagai risiko yang bisa menghambat berjalannya sistem informasi sehingga mengakibatkan kerugian seperti database yang hilang, merusak *system*, mencuri informasi karyawan dan lain sebagainya [3]. Kerugian yang terjadi karena risiko-risiko yang muncul tersebut harus segera diatasi, dengan manajemen risiko.

Secara umum manajemen risiko memegang kendali yang sangat penting dalam membuat kebijakan terkait risiko yang timbul, mendukung pengelolaan risiko teknologi informasi, membantu mengembangkan proses bisnis dan menghasilkan keuntungan, memastikan kenadali terhadap risiko yang efektif, melakukan eliminasi nilai sisa, penghematan biaya serta pengelolaan sumber daya. [4]. Pada dasar nya manajemen risiko sistem informasi begitu penting untuk dilakukan bagi dunia usaha karena melalui implementasi manajemen risiko diharapkan segala risiko yang akan terjadi pada sistem informasi dapat diminimalisir.

Melindungi operasional dari risiko serangan *cyber* terhadap keamanan jaringan komputer merupakan tugas yang besar yang harus dijalankan oleh perusahaan. Keamanan *cyber* memiliki kelemahan dan jika tidak dilindungi dan dipelihara dengan baik akan menimbulkan kerugian berupa hilangnya data, rusaknya sistem server, layanan yang kurang optimal, dan hilangnya objek-objek penting bagi suatu institusi, baik bisnis, organisasi. atau akademis [5]. *NIST Cybersecurity Framework (NIST CSF)* adalah metode yang dapat digunakan untuk melakukan penelitian ini. Dirancang oleh *National Institute of Standards and Technology (NIST),* metode ini mengatasi kurangnya standar terkait keamanan *cyber* dan memberikan seperangkat aturan, pedoman, dan standar yang seragam untuk digunakan organisasi di seluruh industri. *NIST Cybersecurity Framework (NIST CSF)* secara luas dianggap sebagai standar emas untuk membangun program keamanan *cyber* [6]. *Framework* Ini adalah pendekatan yang sangat komprehensi dan progresif terhadap penilaian risiko keamanan TI, berdasarkan identifikasi sistem dan dokumentasi penilaian risiko, dan mencakup semuanya mulai dari mengidentifikasi asal muasal ancaman hingga evaluasi dan penilaian berkelanjutan. *Framework NIST Cybersecurity* sudah digunakan oleh perusahaan manapun baik itu perusahaan kecil, maupun perusahaan besar, karena mudah untuk digunakan, mudah mengetahui gap yang terdapat pada perusahaan, dan implementasi untuk menanggapi gap yang ditemukan[7]. Namun dalam hal ini tetap diperlukannya manajemen risiko teknologi informasi yang berguna untuk mengidentifikasi

risiko, mengukur dampak risiko, dan mengembangkan strategi untuk mengurangi risiko. *Framework NIST Cybersecurity* yang berhubungan dengan *NIST Special Publication* 800-53 memberikan langkah rekomendasi kontrol untuk peningkatan keamanan *cyber* yang ingin dicapai.

PT. XYZ adalah perusahaan manufaktur yang menghasilkan produk berkualitas untuk memenuhi permintaan global yang terus meningkat. Sebagai perusahaan yang terus memiliki perkembangan terbaru, PT. XYZ menciptakan produk berkualitas dan beroperasi dengan mempertimbangkan karyawan, masyarakat, dan lingkungan di mana pun mereka beroperasi. PT. XYZ mencapai hal ini dengan memanfaatkan teknologi dan inovasi, bermitra dengan masyarakat, dan mematuhi standar operasi bisnis internasional di seluruh produksi dan rantai pasokannya. Untuk mendukung penerapan ini, infrastruktur dan aset TI perusahaan sangat penting agar sistem TI dapat memberikan layanan kepada karyawan dan komunitas, serta perkembangan teknologi yang mengharuskan setiap aktivitas. Pekerjaan harus dilakukan pada waktu yang bersamaan dengan dukungan menggunakan internet. Tuntutan akan pengiriman yang aman dan cepat penting untuk produktivitas perusahaan saat ini, yang memerlukan infrastruktur jaringan perusahaan agar tetap tangguh, tersedia, dan aman.

PT. XYZ mempunyai infrastruktur TI yang terbilang lengkap yang dipergunakan untuk memberikan fasilitas kepada karyawan perusahaan, termasuk sistem layanan web dan situs web. Sistem layanan web dan website pada PT. XYZ diklasifikasikan menjadi beberapa sistem layanan internal dan eksternal. Tujuan PT XYZ mengutamakan pelayanannya melalui sistem web *service* dan website karena semua informasi dan data harus dicatat secara digital dan bila diperlukan data tersebut dapat diakses melalui Sistem web *service* dan website.

Beberapa sistem layanan web internal dan eksternal yang digunakan oleh karyawan telah diserang, menyebabkan gangguan sistem seperti serangan

security breaches, indetity theft, malware, email phising, dan dakan ada dampak yang diberikan pada perusahaan. Seperti table yang ada di bawa ini.

Table 1.1 Sistem Keamanan Web Dan Situs Web

Sistem layanan web dan situs web	Kerentanan	Ancaman	Dampak
elearning.xyz.co.id	● Valid Credentials Discovered In Business *System* Via InfoStealer ● ASP.NET Debug Mode Enabled ● SQL Injection ● SSL/TLS CBC Mode Ciphers Supported	● *Data theft* ● *Security breaches* ● *Malicious code*	Hilang nya data training internal employee,risiko terjadi nya penyebaran data
Company Profile	● TLS 64-bit Block Size Cipher Suites Supported ● SSL/TLS CBC Mode Ciphers Supported ● SSL/TLS RC4 Cipher Suites Supported	● *Security breaches* ● *Data theft*	*Data company tercuri*

Sistem layanan web dan situs web	Kerentanan	Ancaman	Dampak
Development Access Cabang A	● PHPInfo Discloses Sensitive Environmental Variables	● *Data theft* ● *Malicious code*	Aplikasi development untuk penjualan di retas

Framework NIST Cybersecurity telah digunakan secara luas oleh peneliti-peneliti sebelumnya. Seperti yang dilakukan oleh (Victor Ilyas Sugara, Hadi Syahrial, Muhammad Syafrullah 2019) menggunakan framework NIST Cybersecurity untuk memeriksa system keamanan siber infrastruktur di perusahaan apakah sudah memenuhi standar atau belum. Penelitian (Kamalanathan Kandasamy, Sethuraman Srinivas, Krishnashree Achuthan & Venkat P. Rangan, 2020) menggunkan framework NIST Cybersecurity untuk memeriksa risk assessment yang ada pad IoT. Terdapat persamaan dan perbedaan dalam penelitian yang terdahulu dengan penelitian yang dilakukan pada saat ini. Persamaan penelitian terdahulu dengan penelitian yang sekarang ialah memakai framework NIST Cybersecurity untuk melakukan peningkatan keamanan siber. Sedangkan perbedaan penelitian terdahulu dan penelitian yang dilakukan saat ini adalah, ruang lingkup penelitian yang berbeda dan penelitian ini menggunakan *tools* vulnerability scanning yaitu WatchTowr sebagai alat untuk mengidentifikasi kerentanan pada setiap sistem operasi web dan situs web sehingga setiap sistem operasi web dan situs web dapat meningkatkan keamanannya. Selain itu penelitian saat ini akan dilakukan penentuan prioritas pada penanganan setiap serangan yang masuk.

Ketika serangan *cyber* terjadi, penanganan terhadap serangan tidak bisa dilakukan dengan cepat karena masih belum ada nya prioritas dalam penanganan masalah yang masuk, seperti penanganan beberapa website yang memiliki prioritas risiko tinggi ditangani di akhir dan website yang memiliki

prioritas risiko rendah di tangani terlebih dahulu. Hal ini menyebabkan terganggunya aktivitas yang ada di perusahaan. Setelah mengetahui permasalahan yang terjadi maka akan dibuat penilaian untuk meningkatkan keamanan *cyber* dan skala prioritas layanan web, sehingga dibutuhkan penerapan *Framework NIST Cybersecurity* untuk membantu lankah-langkah penelitian dan menjadi modul dasar dalam penilaian.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan, maka berikut merupakan rumusan masalah yang akan diselesaikan pada penelitian ini

1. Bagaimana menentukan prioritas risiko ancaman di PT. XYZ?
2. Rekomendasi apa yang hendak dipakai untuk membantu mengoptimalkan manajemen risiko pada PT XYZ ?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah dipaparkan di atas, terdapat batasan-batasan tertentu seperti:

1. Penelitian Manajemen Risiko Keamanan Sistem Informasi ini dilakukan pada divisi IT Security PT XYZ.
2. Kerangka kerja yang akan digunakan pada penelitian ini adalah *Framework NIST Cybersecurity* dan mengambil rekomendasi dari NIST SP 800-53

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

1. Menentukan tingkat level prioritas ancaman yang masuk, sehingga bisa memprioritaskan ancaman berdasarkan tingkatan level.
2. Memberikan rekomendasi untuk mengoptimalkan keamanan sistem informasi pada PT. XYZ berdasarkan *NIST Cybersecurity Framework.*

1.4.2 Manfaat Penelitian

Manfaat dari dibuatnya penelitian ini adalah:

1. Dapat digunakan sebagai referensi untuk melakukan penilaian risiko manajemen menggunakan kerangka kerja *NIST Cybersecurity* di perusahaan ataupun di institusi pemerintahan lainnya.
2. Memberikan hasil penilaian risiko manajemen pada sistem informasi yang dianalisa pada PT. XYZ
3. Menigkatkan keamanan sistem informasi PT. XYZ

1.5 Sistematika Penulisan

Sistematika penulisan yang diterapkan pada skripsi ini terbagi dalam lima bab:

BAB I PENDAHULUAN

Dalam bab pendahuluan berisi mengenai latar belakang masalah, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan adanya sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Dalam bab tinjauan pustaka membahas keseluruhan dari teori-teori yang dijadikan pengetahuan dasar dalam pengerjaan penelitian untuk mengukur tingkat kapabilitas.

BAB III

METODOLOGI PENELITIAN Dalam bab metodologi penelitian membahas objek studi, metode studi, variable studi, dan teknik pengumpulan data dalam penelitian yang akan digunakan.

BAB IV

ANALISIS DAN PENELITIAN

Dalam bab analisis dan penelitian membahas bagian berisikan pembahasan dari hasil proses yang didapatkan, dan menentukan pada level manakah domain yang sudah terpilih berada.

BAB V PENUTUP

Pengukuran Tingkat Kapabilitas Dalam bab penutup berisikan kesimpulan dari hasil audit yang sudah dilakukan yaitu capability level yang ada pada PT XYZ, beserta berisikan saran yang didapatkan dari hasil dan pembahasan.