BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Di era digital saat ini, data telah menjadi aset paling berharga bagi perusahaan. Hampir seluruh aktivitas bisnis, mulai dari operasional harian hingga pengambilan keputusan strategis, bergantung pada integritas dan ketersediaan data. Namun, seiring dengan meningkatnya ketergantungan terhadap teknologi informasi, ancaman terhadap keamanan data juga semakin kompleks dan berbahaya. Salah satu ancaman paling merusak adalah serangan ransomware, yaitu jenis malware yang mengenkripsi data korban dan menuntut tebusan untuk pemulihannya [1].

Dampak dari serangan ransomware tidak hanya terbatas pada hilangnya data, tetapi juga menyebabkan *downtime* operasional yang signifikan, kerugian finansial, dan kerusakan reputasi perusahaan. Berdasarkan laporan industri, waktu rata-rata pemulihan pasca serangan ransomware dapat mencapai 24 hari, yang tentunya berdampak besar terhadap produktivitas dan layanan bisnis. Bahkan, sektor-sektor kritis seperti *healthcare* dan *financial services* mencatat kerugian rata-rata masing-masing sebesar USD 7.42 juta dan USD 5.56 juta akibat pelanggaran data, menjadikannya industri dengan biaya pelanggaran tertinggi selama lebih dari satu dekade [2, 3].

Salah satu perusahaan teknologi yang telah lama berkontribusi dalam pengembangan solusi keamanan data adalah International Business Machines (IBM). Perusahaan ini didirikan pada tahun 1911 di Amerika Serikat dengan nama awal *Computing-Tabulating-Recording Company (CTR)*, kemudian berganti nama menjadi IBM pada tahun 1924 dan berkembang menjadi salah satu pelopor utama dalam industri teknologi informasi global. Dengan pengalaman lebih dari satu abad, IBM terus bertransformasi untuk menjawab tantangan teknologi modern, termasuk menghadirkan solusi tangguh untuk meningkatkan *cyber resilience* perusahaan terhadap ancaman siber seperti ransomware [4].

Untuk menghadapi ancaman ini, perusahaan perlu mengadopsi pendekatan *cyber resilience*, yaitu kemampuan sistem untuk tetap berfungsi dan pulih dengan cepat setelah mengalami gangguan atau serangan. *Cyber resilience* tidak hanya berfokus pada pencegahan, tetapi juga pada pemulihan cepat dan efektif dari insiden

keamanan [5].

Salah satu teknologi yang mendukung strategi ini adalah IBM Safeguarded Copy, sebuah solusi proteksi data yang dirancang untuk menghadapi ancaman siber, termasuk ransomware. Teknologi ini memungkinkan pembuatan salinan data yang bersifat *immutable* (tidak dapat diubah atau dihapus), disimpan secara terisolasi, dan hanya dapat diakses melalui proses yang terkontrol. Dengan fitur seperti *rapid recovery*, integrasi dengan *automation tools*, serta dukungan terhadap berbagai sistem keamanan, IBM Safeguarded Copy memberikan lapisan perlindungan tambahan yang sangat penting dalam menjaga kontinuitas bisnis [6].

Keunggulan utama dari IBM Safeguarded Copy antara lain:

- **Immutability**: Salinan data bersifat *read-only* dan tidak dapat dimodifikasi, sehingga aman dari manipulasi.
- **Cyber resilience**: Dirancang untuk mendukung pemulihan cepat dari serangan siber.
- **Rapid recovery**: Waktu pemulihan jauh lebih cepat dibandingkan metode tradisional, bahkan hanya dalam hitungan jam.
- **Integrasi dengan automation dan security tools**: Memungkinkan pengelolaan salinan data secara otomatis dan aman [4].

Berdasarkan latar belakang tersebut, pelaksanaan magang difokuskan pada eksplorasi dan pengujian teknologi IBM Safeguarded Copy untuk mengukur ketahanan sistem penyimpanan terhadap serangan *ransomware*, serta efektivitas pemulihan data dengan cepat (kurang dari 1 menit) apabila terjadi insiden.

1.2 Maksud dan Tujuan Kerja Magang

Pelaksanaan magang ini bertujuan untuk mengimplementasikan keterampilan teknis (*hard skills*) dan non-teknis (*soft skills*) yang diperoleh selama perkuliahan ke dalam dunia kerja. Selain sebagai pemenuhan kewajiban akademik, magang ini difokuskan pada peningkatan pemahaman dan keterampilan dalam bidang keamanan data dan proteksi sistem, khususnya melalui penerapan teknologi IBM Safeguarded Copy untuk menguji ketahanan sistem penyimpanan terhadap serangan *ransomware*.

Jobdesk magang mencakup pemahaman kebutuhan pelanggan, seperti mengidentifikasi kapasitas penyimpanan data (dalam terabyte/TB), menentukan

performa *storage* (IOPS), serta menganalisis target *Recovery Time Objective (RTO)* dan *Recovery Point Objective (RPO)* untuk pemulihan data. Peserta juga bertanggung jawab dalam konfigurasi sistem *storage*, termasuk pemilihan tipe IBM Storage, jumlah dan tipe *drive*, serta perhitungan kapasitas dan performa.

Tahap implementasi dilakukan melalui *Proof of Concept (PoC)*, meliputi konfigurasi dasar sistem virtual (LPAR/VM), instalasi dan pengaturan sistem operasi serta jaringan, pembuatan kebijakan *backup* dan retensi data, serta pengujian fitur Safeguarded Copy melalui simulasi serangan *ransomware*. Peserta juga terlibat dalam pemantauan status *snapshot* dan validasi integritas data.

Tahap akhir mencakup pengujian dan evaluasi, yaitu melakukan simulasi serangan *ransomware* untuk mengukur efektivitas proteksi, kecepatan pemulihan (RTO), dan akurasi data (RPO). Seluruh rangkaian kegiatan ini dirancang untuk memastikan pemahaman teknis yang mendalam dan efektivitas solusi dalam skenario nyata.

Hasil yang Diharapkan

Melalui berbagai tugas tersebut, diharapkan peserta magang dapat:

a) Memahami ruang lingkup pekerjaan di bidang teknologi informasi, mencakup perangkat keras (*hardware*), perangkat lunak (*software*), dan solusi berkelanjutan (AI, *Machine Learning*, *Data Protection*, dsb).

b) Memahami proses kerja profesional dan meningkatkan pengalaman kerja kolaboratif dalam tim, baik internal perusahaan maupun eksternal (mitra bisnis dan pelanggan).

c) Meningkatkan pengetahuan terkait teknologi penyimpanan data (*storage system*) meliputi *data protection* dan ketahanan sistem terhadap serangan siber.

d) Melakukan analisis keamanan sistem, termasuk pengujian ketahanan terhadap serangan *ransomware*.

Selain itu, pelaksanaan magang ini juga menjadi sarana untuk mengasah kedisiplinan, tanggung jawab, dan kemampuan komunikasi, yang merupakan aspek penting dalam dunia kerja profesional.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Pelaksanaan kerja magang dimulai dari tanggal 20 Agustus 2025 hingga 20 Januari 2025, sesuai dengan kontrak kerja yang telah disepakati antara pihak perusahaan dan peserta magang. Magang ini dilaksanakan di **PT IBM Indonesia**, berlokasi di The Plaza Office Tower, Lantai 16, Jl. M.H. Thamrin Kav. 28–30, Jakarta 10350.

Selama pelaksanaan magang, peserta didampingi oleh pembimbing lapangan, yaitu Bapak Rekiardi, yang menjabat sebagai *Country Leader, Infrastructure Technical Sales* di IBM Indonesia. Kegiatan magang dilakukan setiap hari kerja (Senin hingga Jumat), mulai pukul 08.00 WIB hingga 18.00 WIB, dan dilaksanakan secara *Work From Office* (WFO) di kantor pusat perusahaan.

Pada minggu pertama, kegiatan diawali dengan sesi *onboarding* yang bertujuan untuk memperkenalkan struktur organisasi perusahaan, sistem kerja, serta penjelasan terkait proyek dan teknologi yang akan digunakan selama magang, khususnya mengenai IBM Safeguarded Copy. Setiap hari, kegiatan dimulai dengan melakukan presensi dan mengisi laporan harian yang mencakup tugas yang telah dikerjakan pada hari sebelumnya (*yesterday tasks*) dan rencana pekerjaan untuk hari tersebut (*today tasks*).

Selama periode magang, peserta terlibat dalam berbagai aktivitas teknis yang relevan, seperti konfigurasi sistem virtual, pengaturan sistem operasi (OS) dan jaringan, implementasi kebijakan *backup*, serta pengujian Safeguarded Copy melalui simulasi serangan *ransomware*. Kegiatan ini dilakukan dalam bentuk *proof of concept* (PoC) untuk memastikan pemahaman teknis dan efektivitas solusi dalam skenario nyata. Selain itu, peserta juga berkontribusi dalam pengaturan keamanan dasar, pemantauan sistem, dan pembuatan laporan aktivitas proteksi data, yang semuanya bertujuan untuk mendukung peningkatan *cyber resilience* perusahaan.