BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Perusahaan pengelolaan air bersih merupakan sebuah perusahaan swasta nasional yang bergerak di bidang pengelolaan air bersih dan air minum untuk pelanggan rumah tangga, lembaga sosial atau non-komersial, industri dan komersial. Perusahaan ini di tetapkan sebagai pengelola sistem penyediaan air minum (SPAM) oleh kementrian pekerjaan umum dan perumahan rakyat Republik Indonesia. Perusahaan ini berperan sebagai mitra Pemerintah Daerah dalam dalam pengelolaan dan penyediaan air bersih. Perusahaan ini di tunjuk oleh Pemerintah Daerah sesuai kontrak kerjasama yang berlangsung antara 10 sampai 15 tahun dan dapat di perpanjang masa kontrak konsesi nya. Dalam mendukung proses bisnis nya, Perusahaan menggunakan teknologi informasi dalam menunjang kinerja Perusahaan kepada pelanggan.

Perkembangan teknologi informasi yang mewajibkan perusahaan menggunakan teknologi informasi dalam menunjang proses bisnis dan peningkatan layanan kepada pelanggan. Perusahaan mengelola dan menyimpan data penting dan rahasia pelanggan dalam sistem informasi yang di kembangkan oleh Perusahaan. Dalam pengelolaan data penting dan rahasia pelanggan, perusahaan sudah menerapkan beberapa langkah dalam meminimalisir risiko terjadi nya kebocoran data pelanggan dan data rahasia Perusahaan.

Keamanan informasi menjadi tanggung jawab Perusahaan di Internasional dan juga di Indonesia, hal ini telah menjadi pusat perhatian dunia dan di Indonesia dalam pengelolaan data pribadi pelanggan. Perusahaan kini diwajibkan untuk melakukan pengelolaan keamanan informasi guna meningkatkan kepercayaan dan reputasi Perusahaan. Saat ini kebocoran data dan pelanggaran privacy semakin sering terjadi sehingga tindakan yang ketat dalam menjaga kerahasiaan dan integritas data menjadi kunci utama untuk memenuhi kewajiban hukum dan membangun hubungan yang lebih kuat dengan pelanggan dalam menciptakan lingkungan bisnis yang aman dan terpercaya.

Menurut sumber website katadata.co.id bahwa Indonesia Masuk dalam 3 Besar Negara dengan Kasus Kebocoran Data Terbanyak Dunia dengan jumlah 12.7 juta akun yang mengalami kebocoran data pada kuartal ke 3 tahun 2022. Hasil Analisa yang

dilakukan oleh Kata Data di website bahwa kasus kebocoran data di Indonesia (Data, 2022) meningkat 143% pada kuartal II 2022, kasus kebocoran data ini berpotensi dapat terjadi di Perusahaan sehingga dapat merugikan perusahaan dan pemilik data tersebut.

Risiko *cyber security* menjadi *top risk* atau risiko tertinggi menurut survey yang dilakukan oleh *Global Survey of Institutes of Internal Auditing* tahun 2024. Sehingga risiko ini perlu menjadi fokus Perusahaan dalam pengelolaan data rahasia pelanggan dan data sensitif perusahaan.

Dalam melindungi data pribadi pelanggan, Pemerintah telah mengeluarkan Undang-Undang nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (PDP) (Informatika, 2022) yang mewajibkan Perusahaan melindungi data pribadi pelanggan. Oleh karena ini, Direksi dan Komisaris sangat kuatir akan terjadi kebocoran data pribadi pelanggan dan data sensitif Perusahaan sehingga perlu strategi untuk melakukan pengelolaan risiko terkait keamanan informasi Perusahaan.

Jenis Kebocoran data yang sering terjadi adalah kebocoran data pribadi, kebocoran data rahasia perusahaan, kebocoran data digital, kebocoran data keamanan, kebocoran dokumen fisik, kebocoran data internal. Hal ini biasa nya disebabkan oleh kurang nya kompetensi pengelola TI, kurang nya kesadaran keamanan pegawai internal, kurangnya pengawasan terhadap pihak ketiga, dari sisi pengelolaan server dapat terjadi karena konfigurasi yang lemah, lemahnya tingkat keamanan password, kerentanan pada aplikasi dan terdapat serangan siber dari luar perusahaan.

Bahkan kebocoran data terjadi pada Pusat Data Nasional karena terdampak ransomware pada juni tahun 2024. Kebocoran data pribadi yang pernah terjadi di dunia seperti Facebook tahun 2018 cambridge analytica mengakses data pribadi jutaan pengguna Facebook tanpa izin dan data tersebut dikumpulkan melalui aplikasi pihak ketiga bernama "*This is your digital life*" sehingga di denda 5 Milliar, kasus Amazon tahun 2021 yang mengalami kebocoran data pribadi pengguna sebanyak 37 juta pelanggan di area Uni Eropa dan data tersebut bocor dari divisi cloud computing amazon yang terjadi karena konfigurasi database yang menyebabkan akses tanpa izin sehingga di denda 886 Juta, dan kasus Didi Global tahun 2019 dimana lebih dari 57 juta data pribadi pengguna bocor dan gagal melindungi data pribadi tersebut dari akses tanpa izin sehingga di denda $1,2 Milliar.

Kebocoran data pribadi pengguna lagi marak terjadi sehingga risiko ini perlu di teliti lebih lanjut agar risiko ini tidak terjadi di Perusahaan.

Kasus serangan Mirai.Botnet semakin meningkat sebanyak 58% dari total insiden siber yang dideteksi oleh sistem threat detection and prevention yang ada di Perusahaan, Mirai.Botnet yang merupakan salah satu malware yang mampu mengubah Internet of Thinks menjadi botnet yang dipakai sebagai senjata dalam melancarkan serangan distributed denial-of-service (DDoS), serangan ini dilakukan dari lingkungan eksternal yang menyerang jaringan komunikasi dan sistem Perusahaan.

Dalam konteks ini, penelitian tesis ini menjadi sangat penting untuk menggali lebih dalam dampak dari kasus kebocoran data pribadi pelanggan yang semakin meningkat dan ancaman keamanan siber. Seiring dengan perkembangan teknologi dan ketergantungan perusahaan pada data teknologi informasi, perlindungan terhadap informasi pribadi pelanggan bukan hanya menjadi tanggung jawab operasional semata, melainkan juga menjadi elemen kunci dalam strategi keseluruhan perusahaan.

Dari latar belakang ini, saya mengangkat topik tesis terkait Manajemen Risiko Keamanan Informasi pada Sistem Informasi Pelanggan dan Billing Perusahaan (Studi kasus perusahaan pengelola air bersih) dengan tujuan dapat memberikan kontribusi yang signifikan terhadap pemahaman dan implementasi langkah-langkah preventif serta responsif untuk meminimalisir risiko keamanan informasi yang semakin kompleks dan seringkali merugikan baik bagi pelanggan maupun reputasi perusahaan.

1.2. PERMASALAHAN

Permasalahan utama terkait dengan risiko keamanan informasi, khususnya dalam hal kebocoran data pelanggan. Beberapa aspek yang dapat diidentifikasi sebagai permasalahan utama melibatkan:

1. Indonesia masuk 3 dalam negara dengan kasus kebocoran data terbanyak di Dunia menurut databoks.katadata.co.id.
2. Regulasi Perlindungan Data Pribadi: Dikeluarkannya Undang-Undang nomor 27 tahun 2022 tentang Perlindungan Data Pribadi (PDP) oleh Pemerintah yang mewajibkan perusahaan untuk melindungi data pribadi pelanggan.

3. Risiko Cyber Security: Survey IIA Global tahun 2024 menunjukkan bahwa risiko keamanan siber dan keamanan data menjadi risiko tertinggi (*top risk*). Risiko ini perlu menjadi perhatian penting bagi Perusahaan dalam melindungi data rahasia dan sensitif perusahaan.
4. Risiko Kebocoran Data: Terdapat peningkatan signifikan (143%) kasus kebocoran data di Indonesia pada kuartal II 2022, kasus kebocoran data sudah terjadi di banyak Perusahaan dan berpotensi dapat terjadi di Perusahaan sehingga Direksi dan Komisaris sangat kuatir akan kebocoran data pribadi pelanggan serta data sensitif Perusahaan ke depan.
5. Kasus serangan Mirai.Botnet semakin meningkat sebanyak 58% dari total insiden siber yang dideteksi oleh sistem threat detection and prevention yang ada di Perusahaan, Mirai.Botnet yang merupakan salah satu malware yang mampu mengubah Internet of Thinks menjadi botnet yang dipakai sebagai senjata dalam melancarkan serangan distributed denial-of-service (DDoS), serangan ini dilakukan dari lingkungan eksternal yang menyerang jaringan komunikasi dan sistem Perusahaan.

1.3. RUMUSAN MASALAH

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengetahui proses bisnis dan tujuan pengelolaan sistem pelanggan dan billing pelanggan?
2. Bagaimana mengidentifikasi dan menganalisis risiko keamanan informasi pada sistem pelanggan dan billing pelanggan?
3. Bagaimana strategi Perusahaan dalam memitigasi risiko keamanan informasi sistem pelanggan dan billing pelanggan sesuai tujuan Perusahaan?

1.4. TUJUAN PENELITIAN

Tujuan dari penelitian ini adalah:

1. Mengetahui proses bisnis dan tujuan pengelolaan sistem pelanggan dan billing pelanggan,

2. Melakukan identifikasi dan analisis risiko keamanan informasi pada sistem pelanggan dan billing pelanggan,
3. Merumuskan strategi mitigasi risiko keamanan informasi sistem pelanggan dan billing pelanggan sesuai tujuan Perusahaan.

1.5. RUANG LINGKUP

Penelitian ini memiliki ruang lingkup sebagai berikut:

1. Manajemen Risiko pada Perusahaan pengelola air bersih dan air minum kepada pelanggan rumah tangga, industri dan sosial.
2. Objek analisa pada Teknologi Informasi dan Keamanan Informasi Sistem Informasi pelanggan dan billing pelanggan Perusahaan.
3. Periode data yang di analisis adalah data, layanan dan transaksi pada tahun 2023 sampai 2024.

1.6. MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah:

1. Memberikan mamfaat kepada pelaku bisnis di industri pengelola dan penyedia air bersih dan air minum tentang implementasi manajemen risiko sistem pelanggan dan billing pelanggan.
2. Memberikan penjelasan terhadap strategi tindakan mitigasi risiko atas kejadian yang tidak diinginkan yaitu kebocoran data pribadi pelanggan, kebocoran data transaksi pelanggan.
3. Meningkatkan kepuasan pelanggan.
4. Mengurangi kerugian perusahaan akibat kebocoran data dan kerugian atas reputasi perusahaan.
5. Memberikan kontribusi terhadap limu pengetahuan terhadap ilmu manajemen risiko untuk penelitian lebih lanjut oleh peneliti.