Salah satu contoh kasus etika buruk yang dilakukan oleh tenaga TI adalah kebocoran data pribadi akibat serangan peretasan di Bank Syariah Indonesia (BSI) pada Mei 2023. Dalam kasus ini, grup ransomware LockBit meretas dan mencuri data sensitif milik bank, termasuk data pribadi 15 juta nasabah serta informasi internal perusahaan seperti dokumen keuangan dan kata sandi. Data tersebut kemudian diunggah dan dijual di dark web, mengakibatkan kerugian reputasi yang besar bagi perusahaan. Meskipun pihak bank berupaya meyakinkan publik bahwa data nasabah aman, kebocoran ini tetap memicu ketidakpercayaan pelanggan terhadap keamanan sistem BSI【8†source】【9†source】.

Untuk mengatasi etika buruk seperti ini, beberapa langkah penting yang dapat dilakukan antara lain:

1. *Peningkatan Keamanan dan Audit Rutin*: Perusahaan perlu memperkuat sistem keamanan data, melakukan enkripsi, dan mengadakan audit keamanan secara berkala untuk mendeteksi kerentanan yang mungkin dieksploitasi peretas.

2. *Pelatihan Etika dan Keamanan untuk Tenaga TI*: Tenaga TI perlu dibekali pelatihan tentang etika profesional, khususnya terkait keamanan data dan tanggung jawab terhadap privasi pengguna.

3. *Pengawasan dan Regulasi yang Lebih Ketat*: Pemerintah perlu memperketat regulasi terkait perlindungan data pribadi, termasuk memberikan sanksi tegas kepada perusahaan yang lalai melindungi data pengguna【10†source】【11†source】.

Langkah-langkah ini akan membantu menciptakan lingkungan TI yang lebih aman dan etis, sehingga bisa mencegah insiden serupa di masa depan.