Risiko kebocoran data apabila bekerja dari rumah

KETEGANGAN geopolitik global, khususnya konflik berterusan di Asia Barat, mendorong banyak organisasi mengaktifkan semula Bekerja Dari Rumah (BDR) bagi mengurangkan tekanan kos dan ketidaktentuan operasi. Langkah ini dilihat mampu memastikan kesinambungan perniagaan serta menjaga kebajikan pekerja dalam keadaan ekonomi yang mencabar.

Namun, di sebalik kelebihan fleksibiliti dan keselesaan, timbul persoalan kritikal tentang keselamatan data organisasi. Apabila sempadan fizikal tempat kerja semakin kabur menyebabkan tahap perlindungan maklumat turut berdepan cabaran baharu.

BDR menuntut tanggungjawab lebih besar dalam mengurus data tanpa kawalan fizikal seperti di pejabat.

Hakikatnya, tahap kesedaran individu memainkan peranan penting dalam menentukan keselamatan data. Tanpa pemahaman yang kukuh, pekerja boleh menjadi titik kelemahan yang membuka ruang kepada eksploitasi siber. Tambahan pula, tanpa mekanisme BDR yang tersusun, risiko kebocoran data bukan sahaja meningkat, malah berpotensi menjadi lebih serius apabila organisasi bergantung kepada sistem berpusat yang terdedah kepada serangan.

Laporan keselamatan siber global menunjukkan kos kebocoran data boleh mencecah jutaan ringgit bagi satu insiden, manakala kes berskala besar boleh mengakibatkan kerugian berbilion ringgit.

Kebocoran data bukan sahaja menjejaskan operasi, malah merosakkan reputasi dan membuka ruang kepada jenayah seperti penipuan serta kecurian identiti. Data menjadi aset bernilai tinggi yang turut diperdagangkan di pasaran gelap dalam era digital.

Berbeza dengan persekitaran pejabat yang lebih terkawal, BDR mewujudkan ekosistem kerja yang terdesentralisasi. Data tersebar merentasi pelbagai peranti, aplikasi dan rangkaian dengan tahap keselamatan yang berbeza. Keadaan ini menyukarkan pemantauan dan meningkatkan risiko kebocoran.

Antara cabaran utama ialah fenomena *'shadow IT'*, iaitu penggunaan aplikasi tidak rasmi oleh pekerja bagi memudahkan tugas harian.

Walaupun bertujuan meningkatkan kecekapan, namun tindakan ini boleh mendedahkan data kepada sistem yang tidak dilindungi. Selain itu, penggunaan peranti peribadi tanpa kawalan keselamatan yang mencukupi turut meningkatkan risiko.

Dalam banyak kes, kesilapan kecil seperti kata laluan lemah atau perkongsian akses boleh membawa implikasi besar.

Model BDR juga mencabar aspek akauntabiliti. Apabila berlaku kebocoran, sukar untuk menentukan punca sebenar sama ada berpunca daripada sistem, individu atau kelemahan polisi. Keadaan ini boleh melambatkan tindakan pembetulan dan meningkatkan risiko berulang.

Sehubungan itu, organisasi perlu beralih daripada pendekatan reaktif kepada proaktif dalam keselamatan data. Mereka perlu membina budaya keselamatan yang menyeluruh, memperkukuh literasi digital pekerja serta menetapkan garis panduan yang jelas.

Dalam masa sama, keseimbangan antara fleksibiliti dan kawalan perlu diurus dengan bijaksana agar tidak menjejaskan produktiviti.

DR. MOHAMAD RIDHUAN MAT DANGI & NORLIZA OMAR
Pensyarah Kanan, Fakulti Perakaunan,
Universiti Teknologi Mara (UiTM)

BEKERJA Dari Rumah (BDR) bukan lagi sekadar pilihan sementara tetapi sebahagian daripada norma kerja baharu.