



Khác biệt nhận thức an toàn thông tin trong tổ chức đang tạo ra loại **rủi ro** mới

Điều gì tạo ra khác biệt nhận thức giữa lãnh đạo và đội ngũ kỹ thuật và tổ chức cần làm gì trước khi xảy ra sự cố thật?

Tác giả: **Phạm Bá Tín** — Chuyên gia An ninh mạng, 405CYSE

78%

lãnh đạo cấp cao cho biết tổ chức không xảy ra sự cố vi phạm dữ liệu

57%

đội ngũ kỹ thuật nói điều tương tự — cùng một tổ chức

21%

chênh lệch nhận thức về cùng một thực trạng



Ảnh minh họa: AI-generated

Cùng 1 thực trạng nhưng 2 cách ghi nhận khác nhau trong 1 tổ chức

Mới đây, báo cáo của Thales Report đã nhắc đến một chỉ số khác biệt nhận thức. Đây là điểm thú vị mà 405CYSE đã từng trực tiếp ghi nhận tại nhiều doanh nghiệp và báo cáo này sẽ đi sâu phân tích để làm rõ các vấn đề xung quanh khái niệm "khác biệt nhận thức an toàn thông tin".

KHÁC BIỆT NHẬN THỨC TRONG AN TOÀN THÔNG TIN GIỮA CÁC CẤP LÀ GÌ?

Là hiện tượng lãnh đạo cấp cao và đội ngũ kỹ thuật, dù cùng thuộc một tổ chức, lại có đánh giá khác nhau về mức độ an toàn thực tế của hệ thống — bắt nguồn từ khác biệt trong cách tiếp nhận, xử lý và báo cáo thông tin rủi ro giữa các cấp quản lý.

Trong một cuộc khảo sát với 3.120 chuyên gia tại 20 quốc gia, mọi cấp nhân sự đều được hỏi cùng một câu: "Tổ chức có từng bị vi phạm bảo mật không?" Câu trả lời khác nhau rõ rệt tùy vị trí người được hỏi.

78% lãnh đạo cấp cao cho biết tổ chức không xảy ra sự cố vi phạm dữ liệu, trong khi con số này ở đội ngũ kỹ thuật chỉ là 57% — chênh lệch 21% về cùng một thực trạng, trong cùng một tổ chức.



Nguồn: Thales 2026 Data Threat Report — 3.120 chuyên gia, 20 quốc gia

Lãnh đạo cấp cao và đội ngũ kỹ thuật đang nắm giữ 2 bức tranh khác nhau về tình trạng an ninh dữ liệu của cùng một tổ chức. Các số liệu thống kê cho thấy lãnh đạo đang thiếu tiếp nhận thông tin về những vi phạm đã thực sự xảy ra tại tổ chức của chính họ.

Khác biệt nhận thức giữa các cấp nhân sự không xuất hiện ngẫu nhiên — mà có nguyên nhân cụ thể mang tính hệ thống.