



## Sự thiếu hụt về kiến thức bảo mật an ninh mạng trong Hệ thống tổ chức Y tế

Các tổ chức y tế đã phải chịu nhiều áp lực trong năm vừa qua và hiện đã đạt đến mức giới hạn của họ.

Một nghiên cứu toàn cầu của Trend Micro cho biết, trong khi nhiều nơi tăng hạn mức chi phí cho việc di chuyển sang hệ thống đám mây trong đại dịch, một số khác lại chú quan về khả năng bảo mật an ninh mạng của họ.



2,556  
nhà lãnh đạo  
28  
quốc gia

### Tăng trưởng trong đầu tư bảo mật đám mây



**88%**

tổ chức xác nhận rằng đại dịch đã đẩy nhanh quá trình chuyển sang hệ thống đám mây



**43%**

Nâng chi phí vốn và chi tiêu vào các dịch vụ đã có hợp đồng



**39%**

Tăng chi phí đào tạo và vận hành

## Các thách thức nằm ngoài dự đoán



**85%** tin rằng họ kiểm soát từ xa được bảo mật an ninh mạng cho môi trường của họ



Chỉ có **49%** tự tin rằng họ hiểu được vai trò của mình trong Mô hình chia sẻ trách nhiệm bảo mật đám mây

Lượng lớn người được phỏng vấn thừa nhận phần lớn khó khăn là trong cách bảo mật khối lượng công việc trên đám mây, nhất là:



**34%** thiết lập và duy trì các chính sách



**32%** vá lỗi và quản lí lỗ hổng bảo mật



**32%** định sai cấu hình hệ thống đám mây

**43%** cho biết sự thiếu kiến thức là vấn đề lớn trong việc chuyển sang hệ thống đám mây

**40%** cho rằng việc tìm đúng chuyên gia an ninh có kỹ năng phù hợp là một thử thách

**37%** cho biết họ gặp khó khăn tuyển được nhân sự có thể tiến hành bảo mật trên cả hệ thống máy tại chỗ và trên đám mây

Trong khi nhiều tổ chức toàn cầu tận dụng và chuyển sang hệ thống đám mây, họ vẫn còn thiếu sự hiểu biết về cách bảo mật cho nó. Bài nghiên cứu toàn cầu của Trend Micro nêu bật lên khái niệm sai lầm có thể dẫn đến kết quả rò rỉ thông tin nghiêm trọng, đồng thời đưa ra lời đề nghị: Hãy chọn phương án bảo mật thực tiễn nhất cho đám mây và khi chuyển sang hệ thống đám mây.



Để biết thêm thông tin, hãy truy cập [trendmicro.com](https://trendmicro.com)

