**Bài tập nhóm chương 3**

Danh sách thành viên nhóm

**Tình huống**

Ban Giám đốc của một tổ chức dịch vụ tài chính quốc tế đang xem xét kế hoạch sáp nhập bí mật.

CIO nhận được một email đòi tiền chuộc từ một nguồn không xác định nói rằng họ biết về kế hoạch sáp nhập và có thông tin cá nhân của 150.000 khách hàng. Một mẫu chi tiết cá nhân của 500 khách hàng đã được đưa vào email đòi tiền chuộc làm "bằng chứng".

Tổ chức phải trả khoản tiền chuộc đáng kể bằng Bitcoin. Nếu không, kế hoạch sáp nhập sẽ bị công bố và thông tin khách hàng sẽ bị bán công khai trên mạng.

**Yêu cầu**

1. Tài sản bị thiệt hại, nguyên tắc bảo mật bị vi phạm, thiệt hại?
2. Phương thức tấn công?

**Xử lý tình huống:**

1. Ứng phó

* ….
* …..
* ….

*Gợi ý: Phân tích, giảm thiểu thiệt hại, truyền thông,…*

1. Khắc phục

-…

-…

*Gợi ý: Phân tích thiệt hại 🡪 biện pháp khắc phục*

**Bài học kinh nghiệm:**

1. Bảo vệ

-…

-….

*Gợi ý: Kiểm soát truy cập, nhận thức và đào tạo, bảo mật dữ liệu, quy trình, thủ tục bảo vệ thông tin, bảo trì, công nghệ/dịch vụ bảo mật*

1. Phát hiện

* ….
* …

*Gợi ý: Phát hiện các thao tác bất thường, giám sát liên tục an ninh, quy trình phát hiện*