Đề bài tập: Hãy đề xuất chiến lược QLRR ATTT cho một rủi ro CNTT mà bạn biết.

A. Bài làm mẫu để tham khảo

Một sinh viên đề xuất:

Đề xuất kết hợp 2 chiến lược QLRR ATTT đối với rủi ro về bảo mật khi làm việc từ xa kết nối về nơi làm việc qua mạng wi-fi công cộng *(xem thêm cách trình bày bài giải theo dàn bài ở phần B – trang 4 tài liệu này)***.**

I. NHÓM YÊU CẦU – YÊU CẦU THEO PHỤ LỤC A - ISO 27001:2013:

Rủi ro thuộc về 2 nhóm sau:

1. *Nhóm A.6 'Organization of information security', Yêu cầu A.6.2 'Mobile Devices and Teleworking'*
2. *Nhóm A.13 'Communications security', Yêu cầu A.13.1 'Network security management' và A.13.2 'Information transfer'*

II. ĐIỀU KHOẢN VI PHẠM

Người kiểm tra ATTT đã phát hiện sự không phù hợp tại điều khoản sau:

1. **A.6.2.2 Teleworking**
   Control: 'A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.'
2. **A.13.1.1 'Network controls'**
   Control: 'Networks shall be managed and controlled to protect information in systems and applications.'
3. **A.13.1.2 'Security of network services'**
   Control: 'Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced '.

III. NỘI DUNG PHÁT HIỆN VI PHẠM

Tình huống/ngữ cảnh: Nhân viên Công ty XYZ làm việc tại một quán café có tên 'Nguyên Trung', sử dụng thiết bị cá nhân (laptop) kết nối từ xa về Công ty qua mạng wifi của quán cafe; có truy cập vào dữ liệu của công ty trong khi làm việc.

1. **ĐIỂM YẾU:**

Mạng Wifi tại quán café không yêu cầu người dùng nhập mật khẩu khi truy cập, cho phép gửi dữ liệu lên mạng truyền ra ngoài mà không mã hoá.

2. **MỐI ĐE DỌA:**

Kẻ tấn công ('hackers')/tin tặc/kẻ xấu có năng lực tấn công mạng.

3. **RỦI RO TIỀM ẨN:**

Khi dùng WiFi công cộng, máy tính của người dùng có thể bị 'hacked' bởi kẻ tấn công/tội phạm mạng/tin tặc, người dùng có thể bị đánh cắp dữ liệu, bị lây nhiễm phần mềm độc hại, bị tấn công nghe lén và đặc biệt là có thể mất tiền trong tài khoản ngân hàng.

4. **KHẢ NĂNG XẢY RA RỦI RO ('Likelihood'):** 100%
5. **HỆ QUẢ ('Impact'/'Consequence')**:

- Dữ liệu của Công ty bị kẻ xấu chiếm đoạt và bị tiết lộ ngoài ý muốn. Công ty phải bồi thường (hàng trăm triệu VN đồng hoặc nhiều hơn) cho khách hàng vì dữ liệu khách hàng bị tiết lộ công khai hoặc phải trả tiền chuộc cho kẻ tấn công đã chiếm đoạt dữ liệu.
- Người dùng có thể bị mất hợp đồng lao động với Công ty.
- Khách hàng không còn tin tưởng vào uy tín của Công ty nếu bị lộ dữ liệu mật.
- Thông tin tài khoản của người dùng bị chiếm đoạt và bị mất tiền trong tài khoản.
- Máy tính của người dùng bị lây nhiễm mã độc lâu dài mà người dùng không biết.
- Người dùng lây nhiễm mã độc vào các máy tính khác tại công ty hoặc các máy khác.
- v.v.

(Gợi ý: Chọn 1 phát hiện trong số nhiều phát hiện trong BT.Ch02 đưa vào BT này để lập chiến lược QLRR)

IV. CHIẾN LƯỢC QUẢN LÝ RỦI RO ATTT

1. Chọn chiến lược QLRR trong 4 chiến lược sau đây:

- Chấp nhận rủi ro ('Risk Retention'): ☐
- Giảm nhẹ rủi ro ('Risk Mitigation'): ☐
- Tránh né rủi ro ('Risk Avoidance'): ☒
- Chuyển giao rủi ro ('Risk Transfer'): ☒

2. Giải thích:

a) Lý do chọn chiến lược:

- Không muốn bị kẻ tấn công xâm nhập vào máy tính riêng bằng mọi bất cứ giá nào.
- Muốn được bồi thường khi (1)bị mất hợp đồng lao động hoặc (2)bị phạt tiền bởi Công ty hoặc (3)bị mất dữ liệu cá nhân có nguyên nhân từ tấn công mạng.

b) Mục tiêu (là gì?):

Bảo vệ việc truy cập và truyền dữ liệu của Công ty và cá nhân an toàn 100%.

c) Biện pháp kiểm soát để kiểm soát rủi ro và thực hiện chiến lược:

Luôn dùng mạng riêng ảo VPN để kết nối mạng công cộng khi làm việc từ xa có kết nối vào mạng công ty kết hợp với mua bảo hiểm an ninh mạng của nhà cung cấp dịch vụ bảo hiểm.

V. KẾ HOẠCH HÀNH ĐỘNG

Các bước triển khai biện pháp kiểm soát rủi ro (hay phương án xử lý rủi ro)	Dự kiến nguồn lực, chi phí để thực hiện	Đơn vị/ cá nhân thực hiện	Lịch trình triển khai	Thời hạn hoàn thành
1) Chiến lược tránh né rủi ro - Triển khai kết nối mạng công cộng qua VPN **Bước 1:** Chọn nhà cung cấp: Chọn một nhà cung cấp VPN uy tín – ví dụ chọn VNPT hoặc Viettel. **Bước 2**: Tiếp nhận thông tin dịch vụ Nhận hướng dẫn về cách cấu hình cài đặt VPN vào máy tính cá nhân thông qua nhà cung cấp. **Bước 3:** Cài đặt phần mềm VPN client Cài đặt vào thiết bị máy tính cá nhân **Bước 4**: Nhập thông tin kết nối VPN Nhập tên nhà cung cấp VPN, tên kết nối, tên máy chủ, loại VPN và thông tin đăng nhập. **Bước 5:** Bảo mật kết nối VPN - Sử dụng Mật khẩu dài ít nhất 12 ký tự, có chữ hoa, chữ thường ký tự đặc biệt và chữ số;	- Nhân viên kỹ thuật của nhà cung cấp dịch vụ cài đặt cho khách hàng thuê dịch vụ VPN; hoặc - Nhân viên CNTT của Công ty hỗ trợ cài đặt hoặc người sử dụng tự cài đặt; - Liên hệ VNPT và Viettel để có giá thuê dịch vụ VPN (mới nhất): *300 000 đ*	Ông: Trần văn A - Nhân viên kỹ thuật của nhà cung cấp dịch vụ cài đặt cho khách hàng thuê dịch vụ VPN của VNPT	Triển khai từ ngày 01/04/2025	1 ngày

- Mã hóa AES 256 bit; - Sử dụng giao thức OpenVPN và IKEv2; - Cập nhật phần mềm VPN thường xuyên; - Kích hoạt Xác thực Đa yếu tố (MFA); - Bật chức năng ghi nhật ký ('logging') để giám sát (thu thập dữ liệu kết nối chi tiết). **Bước 5:** Lưu và Kết nối Nhấp Lưu sau đó chọn kết nối VPN và nhấp vào Kết nối.				
2) Chiến lược chuyển giao rủi ro - Mua bảo hiểm an ninh mạng của Ngân hàng Vietinbank để được bồi thường khi rủi ro xảy ra Tham gia Bảo hiểm An ninh mạng - Cyber Risk qua ứng dụng VietinBank Ipay để được bảo vệ trong suốt 30 ngày kể từ thời điểm đăng ký thuê dịch vụ. Tra cứu giấy chứng nhận điện tử qua trang web: https://myvbi.vn/tra-cuu	3000đ/tháng	Liên hệ tại Phòng Giao dịch Vietinbank	Triển khai từ ngày 02/04/2025	1 ngày

B. Dàn bài trình bày cho bài tập Chương 2:

I. NHÓM YÊU CẦU – YÊU CẦU:
Ghi ra rủi ro thuộc Nhóm nào và Yêu cầu nào trong Phụ lục A ISO 27001:2013
Ví dụ:
Nhóm A.12 "Operations security"
Yêu cầu A.12.1 "Management direction for information security"

II. ĐIỀU KHOẢN VI PHẠM
Người kiểm tra ATTT đã phát hiện sự không phù hợp tại điều khoản sau:
(ghi ra số hiệu, nội dung điều khoản và biện pháp kiểm soát có liên quan trong Phụ lục A - ISO 27001:2013)
Ví dụ:
A.12.1.1 "Documented operating procedures"
"Control: Operating procedures should be documented and made available to all users who need them".

III. NỘI DUNG PHÁT HIỆN VI PHẠM
Tình huống/ngữ cảnh:……

1. ĐIỂM YẾU:
   (ghi ra nội dung điểm yếu đã phát hiện được)
2. MỐI ĐE DỌA:
   (ghi ra nội dung mối đe dọa đã phát hiện được)
3. RỦI RO TIỀM ẨN:
   (ghi ra nội dung sự kiện tiềm ẩn có thể xảy ra gây hại cho doanh nghiệp khi mối đe dọa có thể khai thác được điểm yếu)
4. KHẢ NĂNG XẢY RA RỦI RO:
   (ghi ra nội dung khả năng / xác suất xảy ra): x% hay tần suất xảy ra
5. HỆ QUẢ:
   (ghi ra nội dung hệ quả / tác động hay mức độ nghiêm trọng khi rủi ro xảy ra)

IV. CHIẾN LƯỢC QUẢN LÝ RỦI RO ATTT

1. Chọn chiến lược nào trong 4 chiến lược sau đây: *(đánh dấu 'x' vào 1 hoặc hơn 1 trong 4 chọn lựa)*

- Chấp nhận rủi ro ☐
- Giảm nhẹ rủi ro ☐
- Tránh né rủi ro ☐
- Chuyển giao rủi ro ☐

2. Giải thích:
   a) Lý do chọn chiến lược: .....
   b) Mục tiêu là gì: .....
   c) Biện pháp kiểm soát để kiểm soát rủi ro và thực hiện chiến lược: ……

V. KẾ HOẠCH THỰC HIỆN:

Các bước triển khai biện pháp kiểm soát rủi ro (hay phương án xử lý rủi ro) được thực hiện theo kế hoạch sau	Dự kiến nguồn lực, chi phí để thực hiện	Đơn vị/ cá nhân thực hiện	Lịch trình triển khai	Thời hạn hoàn thành
(ghi ra)	*(ghi ra)*	*(ghi ra)*	*(ghi ra)*	*(ghi ra)*

./.