



TRƯỜNG ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - VNUHCM - UIT

# QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

**Chương 2**  
**Mối đe dọa, Điểm yếu, Các mục tiêu kiểm  
soát và kiểm soát Rủi ro ATTT**

# Nội dung

---

01

Mối đe dọa (Threat)

02

Điểm yếu (Vulnerability)

03

Các mục tiêu kiểm soát và kiểm soát Rủi ro ATTT

# 01

## Mối đe dọa (Threat)



1. Định nghĩa
  2. Sự cố trong định nghĩa mối đe dọa
  3. Các ví dụ về mối đe dọa ...
  4. Cách nhận biết mối đe dọa đối với ATTT
  5. Phân biệt mối đe dọa và rủi ro khi phát biểu
-

## 1.1 Định nghĩa mối đe dọa (Threat)<sup>(1)</sup>

(Nhắc lại Chương 01.)

### ➤ Rủi ro là gì?

#### ***Định nghĩa 1:***

Rủi ro là sự kết hợp **ba yếu tố** ('element'):

- Bắt đầu bằng một **sự kiện tiềm ẩn** ("potential event");
- Kết hợp với **xác suất xảy ra** ("probability or "likelihood") sự kiện;
- Kèm theo **mức độ nghiêm trọng** ("severity") (hay hậu quả "consequence" hoặc tác động "Impact") mà sự kiện gây ra.

## 1.1 Định nghĩa mối đe dọa (Threat)<sup>(2)</sup>

---

(Nhắc lại Chương 01.)

### ➤ Rủi ro là gì?

**Định nghĩa 2 (theo ISO 31000:2018, ISO 27000:2018):**

Rủi ro là tác động/hiệu ứng của sự không chắc chắn (\*) lên các mục tiêu (*'risk is effect of uncertainty on objectives'*).

## 1.1 Định nghĩa mối đe dọa (Threat)<sup>(3)</sup>

---

### ➤ Rủi ro ATTT là gì?

#### **Định nghĩa 1:**

Trong bối cảnh của hệ thống quản lý ATTT, rủi ro ATTT có thể được thể hiện dưới dạng tác động/hiệu ứng của sự không chắc chắn (\*) lên các mục tiêu ATTT (*'In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives' – ISO 27000:2018*).

## 1.1 Định nghĩa mối đe dọa (Threat)<sup>(4)</sup>

---

### ➤ **Rủi ro ATTT là gì?**

#### **Định nghĩa 2:**

Rủi ro ATTT liên quan đến khả năng<sup>(\*)</sup> các mối đe dọa khai thác được điểm yếu (hay lỗ hổng bảo mật) của tài sản thông tin và hệ quả là tổ chức bị tổn hại (vật chất, danh tiếng, uy tín...). *(Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization – ISO 27000:2018).*

:Rủi ro ATTT được đo lường theo sự kết hợp giữa khả năng xảy ra ('likelihood') một sự kiện ('event') và hậu quả ('consequence') của nó.

:xem slide số 27 '**Báo cáo về một mối đe dọa khai thác điểm yếu**'

## 1.1 Định nghĩa mối đe dọa (Threat)<sup>(5)</sup>

---

➤ Mối đe dọa (Threat)

**Nguyên nhân tiềm ẩn** của sự cố không mong muốn, có thể dẫn đến tổn hại cho hệ thống hoặc doanh nghiệp (3.50) (*potential **cause** of an unwanted incident, which can result in harm to a system or organization (3.50)*) (ISO 27000:2018).

.





## 1.1 Định nghĩa mối đe dọa (Threat)<sup>(6)</sup>

---

### ➤ Mối đe dọa (Threat)

Theo định nghĩa trên thì nguyên nhân tiềm ẩn của sự cố không mong muốn là:

- một hành động (Action), hoặc
- một sự kiện (Event), hoặc
- một tình huống (hay hoàn cảnh) (Circumstance)

độc hại có thể **khai thác điểm yếu**, gây tổn hại cho hệ thống hoặc doanh nghiệp.

(\*) Sự cố (“incident”) là những rủi ro (“risks”) đã hiện hữu (thực sự đã xảy ra) (“materialized”, “real”, “appeared in front of someone”).

## 1.2 Sự cố (Incident) trong định nghĩa mối đe dọa

---

- Mối đe dọa ('threat') và Sự cố ('incident')
  - Sự cố ("incident") là những rủi ro ("risks") đã hiện hữu (thực sự đã xảy ra) ("materialized", "real", "suddenly appeared in front of someone").
  - Một sự cố là một sự kiện không được lên kế hoạch ("unplanned event").
  - Sự cố ATTT ("information security incident") là một hoặc một loạt các sự kiện ATTT ("information security events") không mong muốn hoặc bất ngờ có khả năng gây tổn hại đáng kể đến hoạt động của tổ chức và đe dọa ATTT [ISO 27000:2018] (\*)
  - **Mối đe dọa là bất kỳ sự cố nào có thể ảnh hưởng tiêu cực đến tính bảo mật, tính toàn vẹn hoặc tính khả dụng của tài sản(\*)**.

## 1.3 Các ví dụ về mối đe dọa ATTT đứng đầu danh sách<sup>(1)</sup>

---

### ☐ Trí tuệ nhân tạo (AI)

AI là mối đe dọa nghiêm trọng đối với loài người [Elon Musk]

### ☐ Mối đe dọa nội bộ (Insider threats)

Mối đe dọa nội bộ là các nhân viên làm việc cố ý hoặc vô ý lạm dụng quyền truy cập; nhân viên không tuân thủ các quy tắc và chính sách ATTT, cố tình bỏ qua các biện pháp an ninh; né tránh sử dụng các giao thức an ninh mạng, đánh cắp dữ liệu v.v.

### ☐ Quyền truy cập đặc quyền (privileged access rights)

Lạm dụng hoặc sử dụng sai quyền này là mối đe dọa cho an ninh mạng của doanh nghiệp.

## 1.3 Các ví dụ về mối đe dọa ATTT đứng đầu danh sách<sup>(2)</sup>

---

- ☐ Virus máy tính, sâu máy tính (Viruses and worms)
- ☐ Botnets, Drive-by attacks, Ransomware; Exploit kits, Rootkits, Man-in-the-middle, SQL Injection, Cross-site scripting, Malware;
- ☐ Malvertising; Phishing attacks; Spear phishing; Malicious spam;
- ☐ Distributed denial-of-service (DoS/DDoS) attacks;
- ☐ Advanced persistent threat attacks; Social Engineering attack;
- ☐ Compromised web applications and web pages;
- ☐ (còn nữa)

## 1.4 Cách nhận biết mối đe dọa ATTT<sup>(1)</sup>

- Nhận thức về mối đe dọa qua giáo dục (hướng dẫn, đào tạo, huấn luyện...).
- Tài liệu Mô hình hóa mối đe dọa ('Threat modeling') của doanh nghiệp.
- Lập danh sách tài sản CNTT của doanh nghiệp và xác định tài sản thông tin nào phải được bảo vệ; tài sản nào không thể thiếu để hoàn thành mục tiêu.
- Căn cứ vào Phụ lục A – Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu của tiêu chuẩn **ISO 27001:2013, ISO 27002:2013, TCVN ISO 27001:2019.**

ISO/IEC 27001:2013(E)

### Annex A (normative)

#### Reference control objectives and controls

The control objectives and controls listed in [Table A.1](#) are directly derived from and aligned with those listed in ISO/IEC 27002:2013<sup>[1]</sup>, Clauses 5 to 18 and are to be used in context with [Clause 6.1.3](#).

Table A.1 — Control objectives and controls

<b>A.5 Information security policies</b>		
<b>A.5.1 Management direction for information security</b>		
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	<i>Control</i> A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	<i>Control</i> The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
<b>A.6 Organization of information security</b>		
<b>A.6.1 Internal organization</b>		
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	<i>Control</i> All information security responsibilities shall be defined and allocated.
		<i>Control</i>

## 1.4 Cách nhận biết mối đe dọa ATTT<sup>(2)</sup>

---

- Bản tin của Cục ATTT (Bộ Thông tin và Truyền thông) cảnh báo cho doanh nghiệp về các mối đe dọa, các cuộc tấn công của tội phạm mạng và các lỗ hổng bảo mật.
- Căn cứ vào ý kiến của nhà phát triển ứng dụng CNTT và các bên liên quan có sử dụng ứng dụng về mối đe dọa đối với ứng dụng.
- Một số cách khác để nhận biết mối đe dọa:
  - Sử dụng phần mềm chống virus (antivirus software) để phát hiện;
  - Sử dụng nhật ký (log) phát hiện mối đe dọa;
  - Sử dụng hệ thống giám sát tự động (Automated monitoring systems);
  - Căn cứ vào tài liệu là phụ lục của giáo trình này;
  - v.v.

## 1.4 Cách nhận biết mối đe dọa ATTT<sup>(3)</sup>

- Nhận diện mối đe dọa thông qua việc phân loại mối đe dọa theo nguồn gốc:
  1. Mối đe dọa từ bên ngoài từ các tổ chức, cá nhân bên ngoài hoặc thiên tai;
  2. Mối đe dọa từ bên trong là các nhân viên làm việc cho chính doanh nghiệp;
  3. **Mối đe dọa có cấu trúc** là các cuộc tấn công doanh nghiệp của tội phạm mạng có tổ chức là những kẻ có mục đích rõ ràng và biết rõ họ đang làm gì. (Ví dụ: Stuxnet là một dạng “worm” được một tổ chức tạo ra).
  4. **Mối đe dọa phi cấu trúc** được thực hiện bởi những người nghiệp dư và không có mục tiêu cụ thể.

(\*) Việc phân loại như trên có thể được phân tích xuống các cấp chi tiết hơn để nhận diện mối đe dọa cụ thể đối với hệ thống thông tin.

## 1.4 Cách nhận biết mối đe dọa ATTT<sup>(4)</sup>

---

- Sử dụng khuôn khổ phân loại mối đe dọa ('threat classification framework') (như STRIDE, PESTLE hoặc OCTAVE) để xác định một cách có hệ thống các mối đe dọa tiềm ẩn.
- Các kịch bản ('scenarios') mô tả cách các mối đe dọa có thể khai thác lỗ hổng bảo mật trong hồ sơ ứng phó sự cố ATTT của doanh nghiệp.
- v.v.



## 1.5 Phân biệt mối đe dọa và rủi ro khi phát biểu

---

- **Lưu ý về cách phát biểu một mối đe dọa với chủ doanh nghiệp:**
  - Mối đe dọa phải luôn là **cụ thể**, nhìn thấy và có bằng chứng về sự hiện diện;
  - Mối đe dọa không có sự kết hợp khả năng xảy ra và mức độ nghiêm trọng (hay tác động hoặc hậu quả) như rủi ro
- **Cách phát biểu về rủi ro với chủ doanh nghiệp khác với phát biểu về mối đe dọa:**
  - Rủi ro thường là dự đoán, tiềm ẩn mà không hiện diện rõ ràng như mối đe dọa;
  - Rủi ro là sự kết hợp 3 yếu tố là sự kiện tiềm ẩn, khả năng xảy ra và mức độ nghiêm trọng (hay tác động hoặc hậu quả).
  - Nội dung phát biểu rủi ro thường có cụm từ '*có thể*', '*nhiều khả năng xảy ra*' hoặc cụm từ khác có nghĩa tương đương như vậy.

# 02

## Điểm yếu (Vulnerability)

1. Định nghĩa
2. Các ví dụ về điểm yếu
3. Cách nhận biết điểm yếu
4. Báo cáo về một mối đe dọa khai thác điểm yếu
5. Phân biệt điểm yếu và rủi ro khi phát biểu



## 2.1 Định nghĩa điểm yếu<sup>(1)</sup>

---

### ➤ Điểm yếu (weakness or vulnerability)

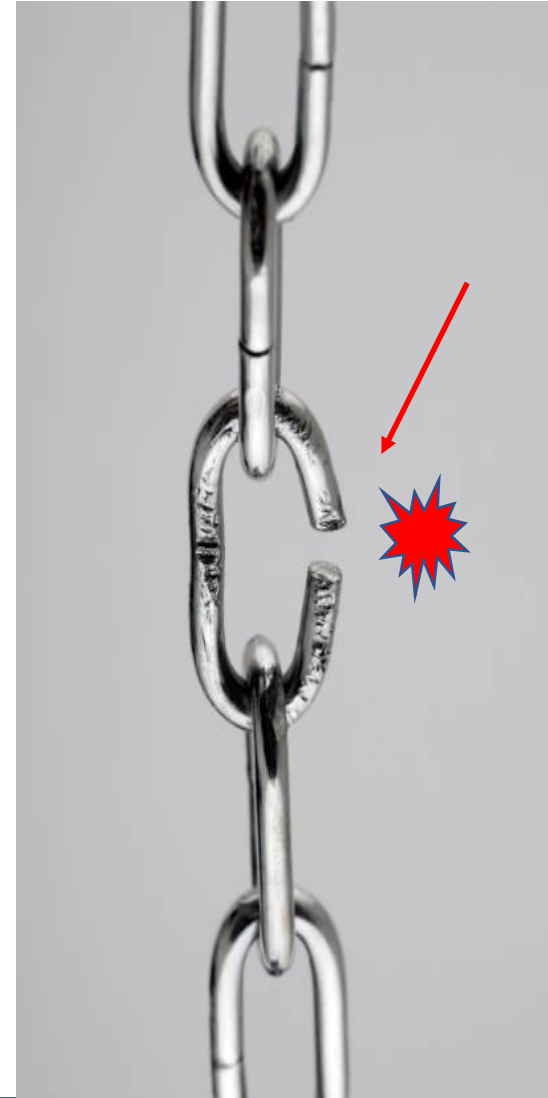
Là điểm yếu của một tài sản hoặc quyền kiểm soát (3.14) có thể bị khai thác bởi một hoặc nhiều mối đe dọa (3.74) (*weakness of an asset or control (3.14) that can be exploited by one or more threats (3.74)*) (ISO 27000:2018).

➤ Một số tài liệu gọi điểm yếu là “*Security hole / Flaw / Error / Bug ...*” đều có hàm ý là “Weakness or Vulnerability” trong ngữ cảnh ATTT.

## 2.1 Định nghĩa điểm yếu<sup>(2)</sup>

### ➤ Điểm yếu (*tiếp*)

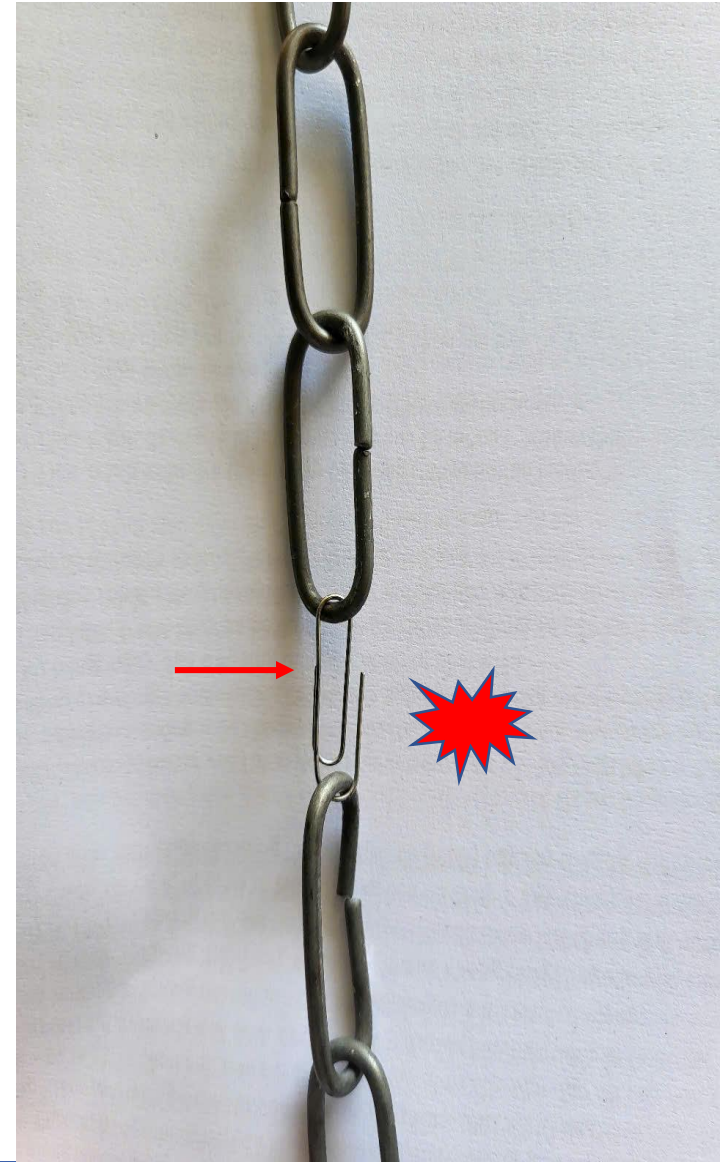
- Theo cách hiểu thông thường thì điểm yếu là những đặc điểm chưa tốt, còn thiếu sót, chưa khắc phục được của con người/hệ thống/ứng dụng CNTT (phần cứng, phần mềm).
- Điểm yếu của con người là thiếu sót về kiến thức, chuyên môn, kinh nghiệm, kỹ năng, tính cách, hành vi....
- Điểm yếu của hệ thống /ứng dụng CNTT thường xuất hiện trong kiến trúc, cấu tạo vật liệu, độ bền, khả năng chịu đựng, năng lực xử lý đồng thời .... yếu kém.



## 2.1 Định nghĩa điểm yếu<sup>(3)</sup>

### ➤ Điểm yếu (Vulnerability)

- Điểm yếu thường được phát biểu kèm theo cụm từ:  
**‘không’, ‘không có’, ‘không tốt’, ‘thiếu’, ‘yếu’, ‘kém’, ‘xấu’, ‘chưa có’, ‘sai’, ‘không đúng’, ‘lỗi hổng’, ‘rạn nứt’, ‘chưa đạt yêu cầu’, ‘chưa được nghiệm thu’, ‘chưa được kiểm tra’, ‘vi phạm’, ‘bị vướng’, ‘bị treo’, ‘cũ/lạc hậu’...** hoặc các từ có nghĩa tương đương như các cụm từ này.



## 2.2 Các ví dụ về điểm yếu<sup>(1)</sup>

---

- ❑ **Không có hoặc thiếu** chính sách/quy định về ATTT trong doanh nghiệp.
- ❑ Ứng dụng được xác thực chỉ bằng mật khẩu (một yếu tố (Single-Factor Authentication)).
- ❑ Ứng dụng sử dụng mật khẩu **yếu** (ít hơn 8 ký tự, không có chữ hoa, ký tự đặc biệt...).
- ❑ Ứng dụng sử dụng giao thức bảo mật **kém** (ví dụ Telnet (thay vì SSH), HPPT).
- ❑ Phần mềm **không** còn được hỗ trợ (không cập nhật bảo mật cho phần mềm).
- ❑ Cấu hình thiết bị mạng ('firewall, router,...') **không** theo chuẩn bảo mật (hay 'best practices').
- ❑ **Không có** thiết bị dự phòng cho ứng dụng quan trọng ('servers, switch,...').
- ❑ **Không có** nguồn điện dự phòng (nguồn dự phòng như máy phát điện).
- ❑ **Không có** hoạt động huấn luyện nâng cao nhận thức ATTT cho nhân viên.
- ❑ Có tài sản loại "public-facing" bị bỏ quên với các cổng mở thường bị kẻ tấn công nhắm mục tiêu (như cổng 80 (HTTP), 443 (HTTPS), 8080 (alternative HTTP), 22 (SSH), 3389 (RDP), or 5900 (VNC)).
- ❑ **Không** áp đặt nghiêm ngặt chính sách nguyên tắc đặc quyền tối thiểu (PoI P).

## 2.2 Các ví dụ về điểm yếu<sup>(2)</sup>

---

- ❑ Hệ điều hành máy tính **không** được hỗ trợ hoặc không được vá lỗi định kỳ (như Windows 7).
- ❑ Danh sách tài sản CNTT **không** được bổ sung, cập nhật kịp thời; hoặc có tài sản bị bỏ quên ('neglected assets') đã lâu, **không** có tên trong danh sách sau nhiều lần cập nhật.
- ❑ Người phụ trách ATTT **không** biết tài sản nào là quan trọng nhất trên hệ thống.
- ❑ **Không có** hồ sơ theo dõi ghi chép các lần cập nhật, vá lỗi phần mềm.
- ❑ Có thông tin xác thực người dùng IAM **không** được sử dụng trong hơn 90 ngày; có vai trò IAM **không** còn sử dụng (identity and access management (IAM)).
- ❑ **Không** áp dụng xác thực đa yếu tố (MFA) cho người dùng là quản trị viên (root user).
- ❑ Dữ liệu DNS **không** được mã hóa, không được xác thực,
- ❑ **Không** có chính sách bảo vệ quyền riêng tư dữ liệu;
- ❑ **Không** xác thực nguồn gốc hoặc xác minh tính toàn vẹn của dữ liệu nhận từ máy chủ DNS;
- ❑ Mật khẩu ngầm định của thiết bị khi xuất xưởng ('factory setting') mà **không** thay đổi;



## 2.2 Các ví dụ về điểm yếu<sup>(3)</sup>

- ❑ **Không** được kiểm tra ATTT định kỳ bởi một tổ chức chuyên đánh giá bảo mật độc lập;
- ❑ **Không có** bất cứ văn bản quy định nào về quản lý mã nguồn ('source code');
- ❑ **Không có** bất cứ văn bản nào quy định về quản lý sự thay đổi ('Change management');
- ❑ **Không có** môi trường kiểm thử phần mềm (ứng dụng) khi tiếp nhận và đưa vào vận hành;
- ❑ **Không có** bất cứ văn bản nào quy định về quản lý thiết bị di động ('smart phone');
- ❑ **Không có** thỏa thuận bảo mật thông tin với các người dùng quan trọng ('admin');
- ❑ Sử dụng bộ định tuyến **cũ** ("second-hand routers") kết nối với mạng thanh toán SWIFT;
- ❑ Giao thức SNMP sử dụng hàm băm MD5 / SHA-1 và thuật toán DES;
- ❑ Hồ sơ **thiếu sót** (thiếu sơ đồ mạng 'Network diagram', danh sách 'users', danh sách IP);
- ❑ Sản phẩm **chưa** được nghiệm thu ATTT;
- ❑ v.v.



## 2.3 Cách nhận biết điểm yếu đối với ATTT<sup>(1)</sup>

---

- Tham khảo tài liệu (danh sách các điểm yếu) để biết về điểm yếu phổ biến.
- Lập danh sách tài sản của doanh nghiệp và xác định điểm yếu của tài sản.
- Điểm yếu còn gọi là lỗ hổng bảo mật trên hệ thống CNTT, ứng dụng CNTT.
- Căn cứ vào Phụ lục A – **ISO 27001:2013, ISO 27002:2013, TCVN ISO 27001:2019** - Các mục tiêu kiểm soát và biện pháp kiểm soát.(\*): **Nếu hệ thống CNTT của doanh nghiệp thiếu hoặc không có biện pháp kiểm soát ('control') phù hợp tại Nhóm Yêu cầu chỉ ra trong Phụ lục, điểm yếu sẽ được nhận diện ngay tại nơi không phù hợp.**

## 2.3 Cách nhận biết điểm yếu đối với ATTT<sup>(2)</sup>

- Danh sách các lỗ hổng bảo mật thông tin được tiết lộ công khai ('Common Vulnerabilities and Exposures (CVE)'):

**Common Vulnerabilities and Exposures (CVE)** is a publicly accessible database that identifies and catalogs known security vulnerabilities in software and hardware. *(CVE là cơ sở dữ liệu có thể truy cập công khai, xác định và lập danh mục các lỗ hổng bảo mật đã biết trong phần mềm và phần cứng.)*

### Lazarus Hackers Exploited Windows Kernel Flaw in Attacks

Feb 29, 2024 Ravie Lakshmanan

Rootkit / Threat Intelligence



The notorious Lazarus Group actors exploited a recently patched privilege escalation flaw in the Windows Kernel as a zero-day to obtain kernel-level access and disable security software on compromised hosts.

The vulnerability in question is [CVE-2024-21338](#) (CVSS score: 7.8), which can permit an attacker to gain SYSTEM privileges. It was resolved by Microsoft earlier this month as part of [Patch Tuesday updates](#).

## 2.3 Cách nhận biết điểm yếu đối với ATTT<sup>(3)</sup>

---

Ví dụ: Mẫu tin sau đây của Cục ATTT (Bộ Thông tin và Truyền thông) cảnh báo cho doanh nghiệp 2 lỗ hổng bảo mật trên thiết bị mạng của hãng Cisco được tra cứu từ CVE:

*“...Một cuộc điều tra phân tích của các chuyên gia bảo mật quốc tế đã phát hiện nhóm tấn công mới có tên UAT4356.... Quá trình điều tra phân tích, các chuyên gia nhận thấy rằng, nhóm tấn công thường triển khai mã độc, thực thi mã từ xa trên thiết bị bị ảnh hưởng. Hai lỗ hổng bị khai thác gồm có CVE-2024-20353 và CVE-2024-20359 đều tồn tại trên ‘Cisco Adaptive Security Appliance Software’ và ‘Cisco Firepower Threat Defense Software’. Trong đó, lỗ hổng CVE-2024-20353 cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, còn CVE-2024-20359 cho phép đối tượng tấn công thực thi mã tùy ý với đặc quyền root...” – đọc thêm ở trang*

<https://vietnamnet.vn/phat-hien-chien-dich-tan-cong-moi-nham-vao-cac-thiet-bi-mang-cisco-2277393.html>

## 2.3 Cách nhận biết điểm yếu đối với ATTT<sup>(4)</sup>

---

- Căn cứ vào tài liệu kỹ thuật hoặc thông báo của nhà sản xuất ứng dụng CNTT (như Cisco, SolarWinds, Sophos, Juniper Networks, v.v.); tìm hiểu ý kiến của các bên liên quan có sử dụng ứng dụng.
- Cách khác nhận biết điểm yếu:
  - Xây dựng và triển khai Quy trình quản lý điểm yếu hệ thống CNTT;
  - Sử dụng công cụ như “Penetration testing, vulnerability scanners, and security audits”;
  - Căn cứ vào tài liệu là phụ lục của giáo trình này;
  - Bản tin của Cục ATTT (Bộ Thông tin và Truyền thông) cảnh báo cho doanh nghiệp các điểm yếu hay lỗ hổng bảo mật trên hệ thống.

## 2.4 Báo cáo về một mối đe dọa khai thác điểm yếu

---

Ví dụ minh họa một mối đe dọa khai thác điểm yếu của thiết bị tường lửa từ một báo cáo của Bộ Tài Chính Mỹ(\*):

- Mối đe dọa từ hành động của kẻ tấn công khai thác lỗi zero-day;
- Điểm yếu của thiết bị tường lửa Sophos;

*Nguồn (Source):*

[Office of Public Affairs | China-Based Hacker Charged for Conspiring to Develop and Deploy Malware That Exploited Tens of Thousands of Firewalls Worldwide | United States Department of Justice](#)

*Baihoc-ve-MoiDeDoa-DiemYeu.pdf*

## 2.4 Báo cáo về một mối đe dọa khai thác điểm yếu (tiếp)

Ví dụ minh họa một mối đe dọa khai thác điểm yếu của thiết bị tường lửa từ một báo cáo của Bộ Tài Chính Mỹ(\*):

➤ Mối đe dọa trong báo cáo của Bộ Tài Chính Mỹ là:

Hacker có tên Guan Tianfeng	<input checked="" type="checkbox"/> / <input type="checkbox"/>
Hành động tấn công bằng mã độc của Guan Tianfeng	<input checked="" type="checkbox"/>
Phần mềm độc hại (mã độc)	<input checked="" type="checkbox"/> / <input type="checkbox"/>
Lây nhiễm mã độc vào thiết bị tường lửa	<input checked="" type="checkbox"/>
Bị mã độc lấy cắp thông tin mật	<input checked="" type="checkbox"/>

➤ Điểm yếu của thiết bị tường lửa Sophos: lỗ hổng zero-day

## 2.5 Phân biệt điểm yếu và rủi ro khi phát biểu

---

- **Lưu ý về cách phát biểu một điểm yếu với chủ doanh nghiệp:**
  - Điểm yếu phải luôn là **cụ thể**, nhìn thấy và có bằng chứng về sự hiện diện;
  - Điểm yếu không có sự kết hợp khả năng xảy ra và mức độ nghiêm trọng (hay tác động hoặc hậu quả) như rủi ro.
- **Cách phát biểu về rủi ro với chủ doanh nghiệp khác với phát biểu về điểm yếu:**
  - Rủi ro thường là dự đoán, tiềm ẩn mà không hiện diện rõ ràng như điểm yếu;
  - Rủi ro là sự kết hợp 3 yếu tố là sự kiện tiềm ẩn, khả năng xảy ra và mức độ nghiêm trọng (hay tác động hoặc hậu quả).
  - Nội dung phát biểu rủi ro thường có cụm từ '*có thể*', '*nhiều khả năng xảy ra*' hoặc cụm từ khác có nghĩa tương đương như vậy.

# 03

## CÁC MỤC TIÊU KIỂM SOÁT VÀ KIỂM SOÁT RỦI RO ATTT

---





# Nội dung

01

Các chính sách ATTT  
(Information security policies)

02

doanh nghiệp  
đảm bảo ATTT  
(Organization of information security)

03

An toàn  
nguồn nhân lực  
(Human resource security)

04

Quản lý tài sản  
(Asset management)

05

Quản lý truy cập  
(Access Control)

06

Mật mã  
(Cryptography)

07

An toàn vật lý và môi trường  
(Physical and Environmental security)

08

An toàn vận hành  
(Operations Security)

# Nội dung (tiếp)

09

An toàn truyền thông  
(Communication security)

10

Tiếp nhận, phát triển  
và duy trì hệ thống  
TT (System acquisition,  
development and  
maintenance)

11

Quan hệ với nhà  
cung cấp  
(Supplier relationships)

12

Quản lý sự cố ATTT  
(Information security  
incident management)

13

ATTT trong quản lý  
liên tục hoạt động  
Information security aspects  
of business continuity  
management

14

Sự tuân thủ  
(Compliance)

# GIỚI THIỆU

## Tiêu chuẩn quốc tế ISO/IEC 27001:2013 (TCVN ISO 27001:2019)<sup>(1)</sup>

- Information technology — Security techniques — Information security management systems — Requirements (CNTT – Kỹ thuật – Hệ thống quản lý ATTT – Các Yêu cầu)
- Nội dung chính:
  1. Phạm vi áp dụng (“Scope”)
  2. Tài liệu viện dẫn (“Normative references”)
  - ★ 3. Thuật ngữ và định nghĩa (“Terms and definitions”)
  4. Bối cảnh của tổ chức (“Context of the organization”)
  5. Sự lãnh đạo (“Leadership”)
  6. Hoạch định (“Planning”)
  7. Hỗ trợ (“Support”)
  8. Vận hành (“Operation”)
  9. Đánh giá hiệu năng (“Performance evaluation”)
  10. Cải tiến (“Improvement”)
- ★ Phụ lục A (“Annex A – Reference control objectives and controls”)  
Thư mục tài liệu tham khảo (“Bibliography”)

# GIỚI THIỆU

## Tiêu chuẩn quốc tế ISO/IEC 27001:2013 (TCVN ISO 27001:2019)<sup>(2)</sup>

- ISO 27001 là tiêu chuẩn quản lý ATTT cung cấp cho các tổ chức/doanh nghiệp một 'framework' (khuôn khổ) có cấu trúc để bảo vệ tài sản thông tin và hệ thống quản lý ATTT ('ISMS') của họ, bao gồm đánh giá rủi ro, quản lý rủi ro và cải tiến liên tục.
- Giấy chứng nhận đáp ứng tiêu chuẩn ISO 27001:2022 đảm bảo với khách hàng, đối tác và các bên liên quan khác rằng cơ sở hạ tầng ATTT của doanh nghiệp đáp ứng được kỳ vọng của họ. Để đạt được chứng nhận ISO 27001, tùy thuộc vào đặc điểm hoạt động của doanh nghiệp, vào kết quả đánh giá rủi ro (xác định, đánh giá, thẩm định và xử lý rủi ro), vào kế hoạch xử lý rủi ro; doanh nghiệp phải nhận diện và đáp ứng tất cả các yêu cầu cốt lõi của ISO 27001.
- ISO 27001 là khuôn khổ thực hành tốt nhất ("best practice framework") được công nhận trên toàn thế giới về hệ thống quản lý ATTT ("Information security management system (ISMS)).
- Lợi ích của ISO 27001:
  - ❑ Giảm thiểu rủi ro về ATTT và quyền riêng tư;
  - ❑ Tiết kiệm thời gian, tiền bạc nhờ quản lý rủi ro, kiểm toán ATTT liên tục;
  - ❑ Kế hoạch xử lý sự cố ATTT chủ động;
  - ❑ Thúc đẩy danh tiếng và xây dựng lòng tin của khách hàng vào doanh nghiệp.

# GIỚI THIỆU

## Tiêu chuẩn quốc tế ISO/IEC 27001:2013 (TCVN ISO 27001:2019)<sup>(3)</sup>

➤ **Information technology — Security techniques — Information security management systems — Requirements (CNTT – Kỹ thuật – Hệ thống quản lý ATTT – Các Yêu cầu)**

➤ **Giải thích tóm tắt nội dung từng đề mục của ISO 27001:2013:**

1. Phạm vi áp dụng (“**Scope**”):

Tiêu chuẩn áp dụng cho mọi tổ chức không phân biệt loại hình, quy mô, ngành nghề kinh doanh...

2. Tài liệu viện dẫn (“**Normative references**”):

Viện dẫn tài liệu ISO 27000 (quy định số phiên bản, quy cách) dùng kèm với tiêu chuẩn này khi áp dụng.

3. Thuật ngữ và định nghĩa (“**Terms and definitions**”):

Định nghĩa thuật ngữ và giải thích ngữ nghĩa các thuật ngữ.

4. Bối cảnh của tổ chức (“**Context of the organization**”):

Xác định các vấn đề nội bộ và bên ngoài có ảnh hưởng đến mục tiêu của hệ thống quản lý ATTT của tổ chức; xác định nhu cầu và mong đợi của các bên liên quan; xác định phạm vi của hệ thống quản lý ATTT trong phạm vi quản lý của tổ chức; và yêu cầu tổ chức thiết lập, triển khai, duy trì và cải tiến hệ thống quản lý ATTT phù hợp với các yêu cầu của tiêu chuẩn.

5. Sự lãnh đạo (“**Leadership**”)

Sự bảo đảm và cam kết của lãnh đạo doanh nghiệp/tổ chức đối với hệ thống quản lý ATTT; với việc ban hành chính sách ATTT và quy định vai trò, trách nhiệm và quyền hạn có liên quan đến ATTT.

# GIỚI THIỆU

## Tiêu chuẩn quốc tế ISO/IEC 27001:2013 (TCVN ISO 27001:2019)<sup>(4)</sup>

- Information technology — Security techniques — Information security management systems — Requirements (**CNTT – Kỹ thuật – Hệ thống quản lý ATTT – Các Yêu cầu**)
- Giải thích tóm tắt nội dung từng đề mục của ISO 27001:2013 (tiếp)

### 6. Hoạch định (“Planning”):

Hoạch định các hành động xử lý rủi ro, xác định các cơ hội, đề ra các mục tiêu ATTT và cách hoàn thành.

### 7. Hỗ trợ (“Support”):

Xác định các nguồn lực (con người, giáo dục, giao tiếp, tài liệu...) phải có cho hệ thống quản lý ATTT.

### 8. Vận hành (“Operation”):

Lập kế hoạch, triển khai và kiểm soát các quy trình để đáp ứng các yêu cầu và mục tiêu về ATTT; để triển khai các hành động được hoạch định (6.); đánh giá rủi ro định kỳ và xử lý rủi ro theo đúng kế hoạch.

### 9. Đánh giá hiệu năng (“Performance evaluation”):

Giám sát, đo lường, phân tích, đánh giá hiệu quả của hệ thống quản lý ATTT; và kiểm toán ATTT định kỳ.

### 10. Cải tiến (“Improvement”):

Hành động khắc phục khi phát hiện sự không phù hợp (vi phạm tiêu chuẩn) trong hệ thống quản lý ATTT; cải tiến liên tục tính phù hợp, đầy đủ và hiệu quả của hệ thống quản lý ATTT.

# GIỚI THIỆU

## Tiêu chuẩn quốc tế ISO/IEC 27001:2013 (TCVN ISO 27001:2019)<sup>(5)</sup>

➤ Information technology — Security techniques — Information security management systems — Requirements (CNTT – Kỹ thuật – Hệ thống quản lý ATTT – Các Yêu cầu)

➤ Nội dung chính:

1. Phạm vi áp dụng (“Scope”)
2. Tài liệu viện dẫn (“Normative references”)
3. Thuật ngữ và định nghĩa (“Terms and definitions”)
4. Bối cảnh của tổ chức (“Context of the organization”)

5. Sự lãnh đạo (“Leadership”) 6. Hoạch định (“Planning”) 7. Hỗ trợ (“Support”)	PLAN	PDCA or plan–do–check–act is a four-step model for carrying out change, a management method, an iterative design, an improvement cycle or PDCA cycle or the Deming cycle
8. Vận hành (“Operation”)	DO	
9. Đánh giá hiệu năng (“Performance evaluation”)	CHECK	
10. Cải tiến (“Improvement”)	ACT	

Phụ lục A (“Annex A – Reference control objectives and controls”)

Thư mục tài liệu tham khảo (“Bibliography”)

## **GIỚI THIỆU Phụ lục A – Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu (Annex A - Reference control objectives and controls) của tiêu chuẩn ISO 27001:2019 / TCVN ISO 27001:2013<sup>(1)</sup>**

- Nội dung Phụ lục A – Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu của tiêu chuẩn TCVN ISO 27001:2019 / ISO 27001:2013. Phụ lục A bao gồm các mục tiêu và biện pháp kiểm soát ATTT cho 14 nhóm ('14 domains (categories)) yêu cầu cho tài sản (hữu hình và vô hình) của doanh nghiệp.

### **Annex A (normative)**

#### **Reference control objectives and controls**

The control objectives and controls listed in [Table A.1](#) are directly derived from and aligned with those listed in ISO/IEC 27002:2013<sup>[1]</sup>, Clauses 5 to 18 and are to be used in context with [Clause 6.1.3](#).

**Table A.1 — Control objectives and controls**



## **GIỚI THIỆU Phụ lục A – Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu (Annex A - Reference control objectives and controls) của tiêu chuẩn ISO 27001:2019 / TCVN ISO 27001:2013<sup>(2)</sup>**

---

### **➤ Cách sử dụng Phụ lục A (Annex A) ISO 27001**

- **Doanh nghiệp đọc các yêu cầu trong Phụ lục A ISO 27001 để nhận ra tất cả các yêu cầu ATTT thuộc 14 Nhóm Yêu cầu (A.5, A.6, A.7, ..., A.18).**
- **Với từng Nhóm Yêu cầu, doanh nghiệp nhận ra tất cả các Yêu cầu và các Điều khoản liệt kê trong từng yêu cầu (bao gồm mục tiêu ('objective') và biện pháp kiểm soát ('control')) mà doanh nghiệp phải đáp ứng để được chứng nhận đạt ATTT theo tiêu chuẩn ISO 27001.**

[Giaithich PhulucA -ISO27001 Nhom-YeuCau-Dieukhoan-MucTieu-BPKiemSoat.pdf](#)

## GIỚI THIỆU Phụ lục A – Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu (Annex A - Reference control objectives and controls) của tiêu chuẩn ISO 27001:2019 / TCVN ISO 27001:2013<sup>(3)</sup>

---

- **Cách triển khai / kiểm toán thực hiện Yêu cầu trong Phụ lục A**
- **Nhân sự CNTT phụ trách ATTT** của doanh nghiệp đọc yêu cầu và hướng dẫn trong Phụ lục A ISO 27001 đối chiếu với nội dung 'Implementation Guidance' ISO 27002 để rà soát, thiết lập, triển khai và nâng cấp tất cả các biện pháp kiểm soát ATTT tại doanh nghiệp.
- **Nhân sự kiểm toán ATTT độc lập** sử dụng Phụ lục A ISO 27001 đối chiếu với nội dung 'Implementation Guidance' ISO 27002 để kiểm tra xem doanh nghiệp có hay không đáp ứng các Mục tiêu ('*objective*'), Biện pháp kiểm soát ('*control*') nêu ra theo từng Yêu cầu trong Phụ lục A dựa vào mức độ triển khai theo hướng dẫn trong nội dung 'Implementation Guidance'.

## GIỚI THIỆU Phụ lục A – Các mục tiêu kiểm soát và biện pháp kiểm soát tham chiếu (Annex A - Reference control objectives and controls) của tiêu chuẩn ISO 27001:2019 / TCVN ISO 27001:2013<sup>(4)</sup>

---

### ➤ Mục tiêu và biện pháp kiểm soát trong Phụ lục A - ISO 27001

Các mục tiêu và biện pháp kiểm soát được liệt kê trong **Bảng A.1 của Phụ lục A của ISO/IEC 27001:2013** được lấy trực tiếp từ và phù hợp với các mục tiêu và biện pháp kiểm soát được liệt kê trong ISO/IEC 27002:2013[1], Điều 5 đến 18 (từ trang 2 đến trang 78) và được sử dụng trong bối cảnh của **Điều 6.1.3 ‘Information security risk treatment’** trong **ISO/IEC 27001:2013 (trang 4)** – (*“The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.”*)

# Các đối tượng sử dụng Phụ lục A ISO 27001 và ISO 27002

## ➤ Các trường hợp sử dụng Phụ lục A - ISO 27001 và ISO 27002

Stt	Đối tượng	Công việc
1	Nhân sự CNTT phụ trách ATTT	Rà soát, thiết lập, triển khai và nâng cấp tất cả các biện pháp kiểm soát ATTT để đáp ứng tất cả yêu cầu ATTT theo ISO 27001 và ISO 27002 <input type="checkbox"/>
2	Nhân sự kiểm toán ATTT	Tìm kiếm sự không đáp ứng ATTT của hệ thống, chỉ ra điểm yếu (lỗ hổng bảo mật), mối đe dọa và rủi ro tiềm ẩn để doanh nghiệp khắc phục: <input checked="" type="checkbox"/>
3	Kẻ tấn công (tin tặc, tác nhân đe dọa, tội phạm mạng v.v.)	Tìm kiếm điểm yếu (lỗ hổng bảo mật) để khai thác điểm yếu nhằm chiếm đoạt thông tin (dữ liệu) <input type="checkbox"/>

# Kiểm toán ATTT sử dụng Phụ lục A ISO 27001 và ISO 27002<sup>(1)</sup>

---

## ➤ Tính huống minh họa:

- Doanh nghiệp XYZ hoạt động trong lĩnh vực tài chính với tên đăng ký là Ngân hàng TMCP XYZ. Theo Nghị quyết của Hội đồng quản trị năm 2007, Tổng Giám đốc Ngân hàng phải thực hiện đánh giá ATTT độc lập tại Ngân hàng để có cơ sở triển khai dự án lấy Chứng Nhận Quốc Tế ISO 27001 - Hệ thống Quản Lý An Toàn Thông Tin (ISMS). Ngân hàng đã thuê một đơn vị kiểm toán ATTT đến Ngân hàng thực hiện hoạt động kiểm toán hiện trạng ATTT tại Ngân hàng. Đơn vị này đã căn cứ vào Phụ lục A – ISO 27001:2013 để rà soát, kiểm tra và đánh giá mức độ đáp ứng ATTT từ đó chỉ ra các rủi ro tiềm ẩn có thể xảy ra cho doanh nghiệp.

# Kiểm toán ATTT sử dụng Phụ lục A ISO 27001 và ISO 27002<sup>(2)</sup>

---

## ➤ Tính huống minh họa:

- Các Slides dưới đây là trích dẫn nội dung trong Báo cáo của đơn vị kiểm toán ATTT tại Ngân hàng XYZ . Báo cáo phân tích khoảng cách chênh lệch giữa hiện trạng ATTT quan sát được tại một doanh nghiệp so với từng yêu cầu trong tiêu chuẩn ISO 27001 (tiếng Anh gọi là “Gap Analysis Report”).
- Đại diện cho đơn vị kiểm toán ATTT tại doanh nghiệp ghi trong Báo cáo gọi là “Người kiểm tra ATTT tại doanh nghiệp”.

## 3.1 Các chính sách ATTT<sup>(1)</sup>

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.5  
Yêu cầu A.5.1 có 2 Điều (A.5.1.1 và A.5.1.2);  
người kiểm tra ATTT tại doanh nghiệp quan sát  
và thấy rằng doanh nghiệp có:*

### 3.1.1 Điểm yếu được phát hiện:

*Doanh nghiệp chưa có chính sách ATTT được  
phê duyệt, chưa được công bố và thông báo cho  
nhân viên và các đối tác bên ngoài có liên  
quan.[A.5.1.1]*

*(\*) Policy [ISO 27000]: Intentions and direction of an organization (3.50), as  
formally expressed by its top management .*





## 3.1 Các chính sách ATTT<sup>(2)</sup>

---

### 3.1.2 Mối đe dọa ATTT được nhận ra:

- *Mối đe dọa nội bộ (nhân viên không biết gì về chính sách ATTT do không được huấn luyện về chính sách ATTT, không hiểu hoặc không có ý thức về ATTT...);*
- *Mối đe dọa bên ngoài như vi phạm pháp luật (Luật An ninh mạng,...) ;*





## 3.1 Các chính sách ATTT<sup>(3)</sup>

### 3.1.3 Rủi ro (Risks):

- Nhân viên thực hiện nhiệm vụ có thể không làm theo cách thực hành ATTT tốt nhất; (\*)
- Doanh nghiệp có thể bị cơ quan pháp luật phạt tiền;
- Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]
- Hệ quả (Consequences):
  - Tài sản của doanh nghiệp có thể bị tổn thất và định lượng được bằng tiền.
  - Mục tiêu chỉ đạo và hỗ trợ ATTT và tuân thủ pháp luật, quy định liên quan có thể bị thất bại.



## 3.2 Tổ chức đảm bảo ATTT – Tổ chức nội bộ<sup>(1)</sup>

Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.6 Yêu cầu A.6.1 có 5 Điều (A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4 và A.6.1.5); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:

### 3.2.1 Điểm yếu được phát hiện:

*Bảng mô tả công việc của cán bộ và nhân viên không quy định rõ nhiệm vụ gì phải làm khi có sự cố bảo mật (ATTT) xảy ra tại cơ quan.[A.6.1.1]*



## 3.2 Tổ chức đảm bảo ATTT – Tổ chức nội bộ<sup>(2)</sup>

### 3.2.2 Mối đe dọa được nhận ra:

- Nhân viên chỉ làm những việc được ghi trong bảng mô tả công việc;
- Sự lơ là hay sao lãng công việc của bộ phận chuyên trách ATTT.(\*)

### MÔ TẢ CÔNG VIỆC

Họ và tên: Vương Đình .....

Chức danh:	Báo cáo trực tiếp cho:	Phòng:	Ngày: dd/mm/yyyy
Nhân viên CNTT	ô. Trần Hải Học - Trưởng bộ phận Mạng	Công nghệ thông tin	

#### Mô tả công việc:

- Hằng ngày chịu trách nhiệm trông coi tài sản của công ty, trong, ngoài khu vực văn phòng, cũng như vận hành các thiết bị \_\_\_\_\_, \_\_\_\_\_ trong Công ty

## 3.2 Tổ chức đảm bảo ATTT – Tổ chức nội bộ<sup>(3)</sup>

---

### 3.2.3 Rủi ro (Risks)

*Kẻ tấn công (như tin tặc) có thể tấn công vào mạng máy tính của doanh nghiệp.*

- *Khả năng xảy ra (Likelihood):  $\neq 0\%$  / [tần suất (ví dụ 2 lần 1 năm)]*
- *Hệ quả (Consequences):*
  - *Nhân viên không biết phải làm gì trong khi cuộc tấn công đang diễn ra;*
  - *Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền;*
  - *Không thể xử lý cá nhân vi phạm quy định ATTT của doanh nghiệp;*
  - *Mục tiêu kiểm soát việc thực hiện công việc và hoạt động ATTT thất bại.*

## 3.2 Tổ chức đảm bảo ATTT – Các thiết bị di động và làm việc từ xa<sup>(1)</sup>

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.6 Yêu cầu A.6.2 có 2 Điều (A.6.2.1, và A.6.2.2); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### 3.2.1 Điểm yếu được phát hiện:

*Doanh nghiệp không có chính sách ATTT đối với thiết bị di động (\*). [A.6.2.1]*

### 3.2.2 Mối đe dọa được nhận ra:

*Nhân viên dùng thiết bị di động cá nhân truy cập được vào mạng doanh nghiệp và xử lý dữ liệu của doanh nghiệp một cách tùy tiện, không an toàn.*



## 3.2 Tổ chức đảm bảo ATTT – Các thiết bị di động và làm việc từ xa<sup>(2)</sup>

---

### 3.2.3 Rủi ro (Risks)

- Nhân viên doanh nghiệp có thể bị mất thiết bị di động khi làm việc bên ngoài, sao chép/ thay đổi dữ liệu của doanh nghiệp vào thiết bị di động cá nhân rồi đồng bộ hóa dữ liệu với hệ thống qua mạng wi-fi công cộng.
- Kẻ xấu có thể chiếm được dữ liệu doanh nghiệp qua mạng wi-fi công cộng.
  - Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất (ví dụ 1 lần trong 10 lần truy cập)]
  - Hệ quả (Consequences):
    - Tài sản của doanh nghiệp bị tổn thất có thể định lượng bằng tiền;
    - Mục tiêu đảm bảo an toàn khi làm việc từ xa và sử dụng thiết bị di động thất bại.



## 3.3 An toàn nguồn nhân lực<sup>(1)</sup>

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.7 có 3 Yêu cầu (A.7.1, A.7.2 và A.7.3) gồm 6 Điều (A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3 và A.7.3.1); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### 3.3.1 Điểm yếu được phát hiện:

*Người lao động không được đào tạo nâng cao nhận thức về ATTT.[A.7.2.2]*



## 3.3 An toàn nguồn nhân lực<sup>(2)</sup>

---

### 3.3.2 Mối đe dọa được nhận ra:

*Người lao động làm việc tùy tiện, không làm theo quy trình của nhà cung cấp hoặc người lao động sắp nghỉ việc sẽ ít hay không còn quan tâm đến quy trình, quy định ATTT.*





## 3.3 An toàn nguồn nhân lực<sup>(3)</sup>

### 3.3.3 Rủi ro (Risks)

*Người lao động có thể gây ra lỗi khi làm sai quy trình hoặc lấy cắp thông tin nhạy cảm hoặc tài liệu kỹ thuật (công thức, bí quyết, phát minh...) của doanh nghiệp.*

- *Khả năng xảy ra (Likelihood):  $<> 0\%$  / [tần suất]*
- *Hệ quả (Consequences):*
  - *Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền;*
  - *Mục tiêu đảm bảo nhân viên nhận thức được và thực hiện trách nhiệm ATTT thất bại.*

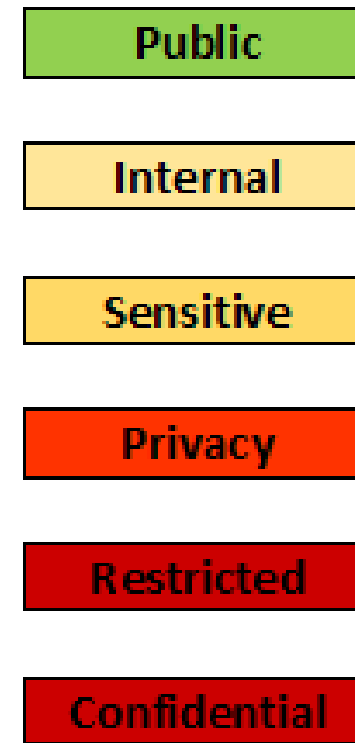


## 3.4 Quản lý tài sản<sup>(1)</sup>

Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.8 có 3 Yêu cầu (A.8.1, A.8.2 và A.8.3) gồm 10 Điều (A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2 và A.8.3.3); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:

### 3.4.1 Điểm yếu được phát hiện:

- a) Không có quy định bàn giao tài sản khi người lao động nhận việc hoặc nghỉ việc.[A.8.1.4];
- b) Không có quy định phân loại thông tin theo mức độ bí mật: mật, tối mật, tuyệt mật.[A.8.2.1].



Information shall be classified in terms of legal requirements,....

## 3.4 Quản lý tài sản<sup>(2)</sup>

---

### 3.4.2 Mối đe dọa được nhận ra:

- a) *Người sử dụng tài sản lạm quyền;*
- b) *Vi phạm bảo mật thông tin.*



## 3.4 Quản lý tài sản<sup>(3)</sup>

---

### 3.4.3 Rủi ro (Risks)

- Có thể mất tài sản khi người lao động nghỉ việc không làm bàn giao;
- Thông tin nhạy cảm của doanh nghiệp có thể bị tiết lộ trái phép.
- Khả năng xảy ra (Likelihood):  $< > 0\%$  / [tần suất (ví dụ 1 người trong 100 người nghỉ việc)]
- Hệ quả (Consequences):
  - Người quản lý để mất tài sản có thể phải bồi thường;
  - Mục tiêu xác định trách nhiệm bảo vệ tài sản thất bại;
  - Mục tiêu đảm bảo thông tin có mức độ bảo vệ phù hợp thất bại;
  - Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền.

## 3.5 Quản lý truy cập<sup>(1)</sup>

---

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.9 có 4 Yêu cầu (A.9.1, A.9.2, A.9.3 và A.9.4) gồm 14 Điều (A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3,..., A.9.2.6, A.9.3.1, A.9.4.1,..., và A.9.4.5); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### 3.5.1 Điểm yếu được phát hiện:

- a) Không có hay chưa ban hành văn bản chính sách, quy trình kiểm soát truy cập;[A.9.1.1];*
- b) Không có hệ thống (ứng dụng) quản lý mật khẩu để đảm bảo sử dụng mật khẩu có chất lượng (về độ dài, độ phức tạp và tính duy nhất).[A.9.4.3].*

## 3.5 Quản lý truy cập<sup>(2)</sup>

### 3.5.2 Mối đe dọa được nhận ra:

- a) Lạm dụng quyền truy cập; trộm cắp thông tin;*
- b) Bị chiếm đoạt (bẻ khóa) mật khẩu bởi tội phạm mạng có năng lực .*





## 3.5 Quản lý truy cập<sup>(3)</sup>

### 3.5.3 Rủi ro (Risks)

- Có thể cấp sai quyền truy cập hay cấp sai quyền truy cập đặc quyền cho người dùng;
- Có thể mất ATTT do mật khẩu bị chiếm và sử dụng trái phép bởi tin tặc.

➤ Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]

➤ Hệ quả (Consequences):

- Người phụ trách ATTT cho hệ thống gặp rủi ro có thể bị mất việc;
- Mục tiêu giới hạn quyền truy cập đối với người dùng thất bại;
- Mục tiêu ngăn chặn truy cập trái phép vào hệ thống và ứng dụng thất bại;
- Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền.

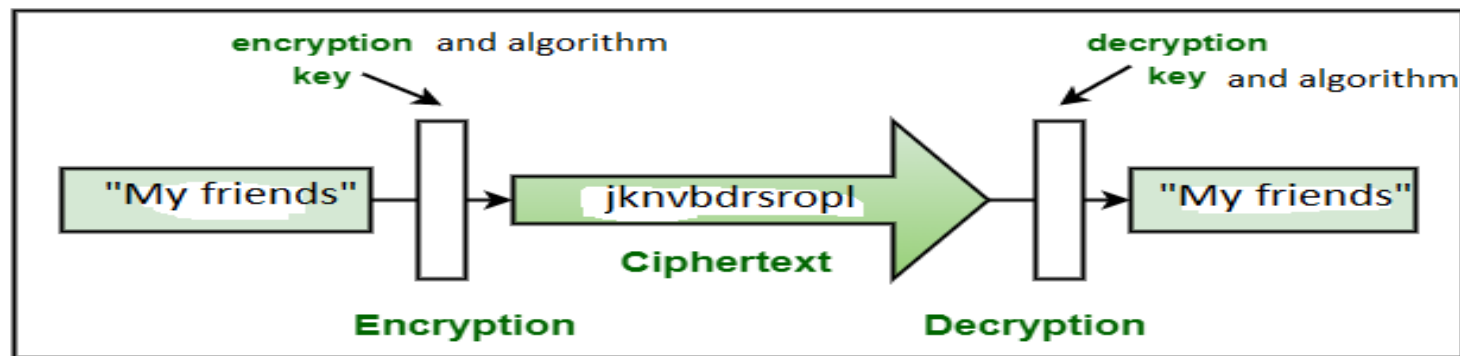


## 3.6 Mật mã<sup>(1)</sup>

Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.10 có Yêu cầu (A.10.1) gồm 2 Điều (A.10.1.1 và A.10.1.2); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:

### 3.6.1 Điểm yếu được phát hiện:

Doanh nghiệp có sử dụng mật mã (“cryptography”) nhưng chưa có chính sách sử dụng mật mã để bảo vệ tính bảo mật (C), tính toàn vẹn (I) và tính xác thực (A) của thông tin; [A.10.1.1]





## 3.6 Mật mã<sup>(2)</sup>

---

### 3.6.2 Mối đe dọa được nhận ra:

*Hành động vi phạm các biện pháp bảo vệ bằng mật mã của doanh nghiệp từ các cá nhân có kỹ năng, kỹ thuật máy tính (như nhân viên nội bộ /hackers/ attackers)*



## 3.6 Mật mã<sup>(3)</sup>

---

### 3.6.3 Rủi ro (Risks)

*Thuật toán mã hóa (cryptographic engine), khóa (private key) hoặc các thông tin nhạy cảm khác của doanh nghiệp có thể bị đánh cắp trái phép (nhân viên nội bộ, người bên ngoài hay bên thứ ba).*

➤ *Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]*

➤ *Hệ quả (Consequences):*

*- Bị lộ hoặc bị đánh cắp bí quyết kinh doanh và các thông tin nhạy cảm do doanh nghiệp chưa có trang bị bảo mật thông tin (như thiết bị Hardware Security Module) để bảo vệ thông tin nhạy cảm.*

## 3.6 Mật mã<sup>(4)</sup>

---

### 3.6.3 Rủi ro (Risks)

- *Hệ quả (Consequences): (tiếp)*
- *Người phụ trách ATTT cho hệ thống gặp rủi ro có thể bị mất việc hay bị truy tố;*
  - *Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền;*
  - *Mục tiêu bảo vệ tính bí mật, tính toàn vẹn, tính xác thực của thông tin thất bại.*



## 3.7 An toàn vật lý và môi trường<sup>(1)</sup>

---

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.11 có 2 Yêu cầu (A.11.1 và A.11.2) gồm 15 Điều (A.11.1.1,..., A.11.1.6, A.11.2.1,..., và A.11.2.9); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### 3.7.1 Điểm yếu được phát hiện:

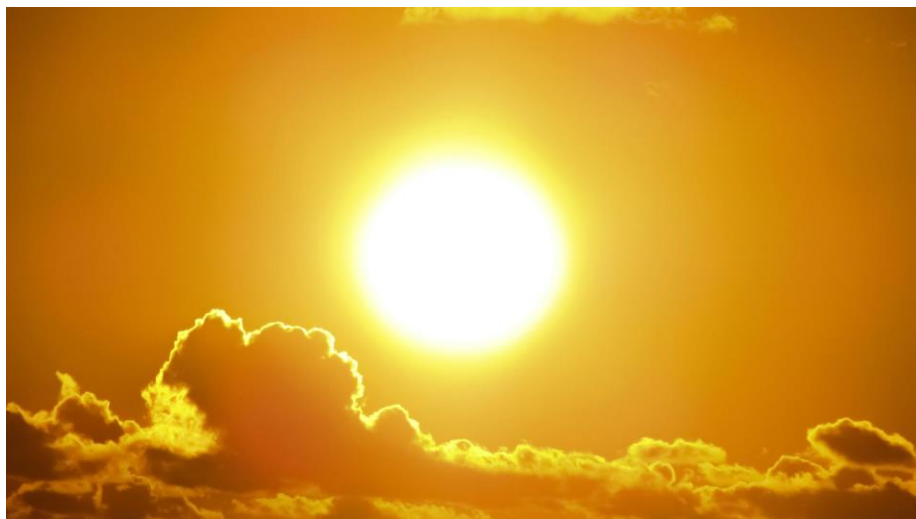
- a) Chưa có biện pháp kiểm soát việc ra vào phòng máy chủ (server room) (thiết bị quét vân tay, thẻ ra vào, nhập số PIN vào thiết bị Terminal tại cửa ra vào...); [A.11.1.3]*
- b) Không đặt cable mạng vào ống bảo vệ (PVC) khi đi dây ngoài trời; [A.11.2.3]*
- c) Bố trí phòng đặt máy chủ trên nền đất thấp tại khu vực hay ngập nước khi trời mưa hoặc ở khu vực có triều cường. [A.11.1.4]*

## 3.7 An toàn vật lý và môi trường<sup>(2)</sup>

---

### 3.7.2 Mối đe dọa được nhận ra:

- a) *Người không có phận sự tùy tiện ra vào phòng máy chủ;*
- b) *Ánh nắng mặt trời rọi trực tiếp vào dây cable;*



## 3.7 An toàn vật lý và môi trường<sup>(3)</sup>

---

### 3.7.2 Mối đe dọa được nhận ra:

*c) Lũ lụt do triều cường, nước mưa tràn vào nhà gây ngập phòng máy chủ.*





## 3.7 An toàn vật lý và môi trường<sup>(4)</sup>

---

### 3.7.3 Rủi ro (Risks)

- a) Thiết bị có thể gặp sự cố vận hành nếu ai đó đụng chạm bất cẩn vào thiết bị; có thể mất các thiết bị di động, tài liệu; sử dụng thiết bị trái phép; làm hỏng phương tiện thông tin; chụp ảnh;
  - b) Dây cable phơi trực tiếp dưới ánh nắng mặt trời lâu ngày có thể bị hư hỏng phần vỏ nhựa bọc lõi đồng làm tăng tiếp xúc phần lõi;
  - c) Nước (mưa) chảy vào phòng máy chủ có thể gây chập mạch điện.
- Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]

## 3.7 An toàn vật lý và môi trường<sup>(5)</sup>

---

### 3.7.3 Rủi ro (Risks)

➤ *Hệ quả (Consequences):*

- *Hệ thống CNTT không vận hành bình thường nếu bị tác động sai;*
- *Mất tín hiệu trên đường truyền (hệ thống bị treo, ngưng hoạt động);*
- *Nước làm hỏng thiết bị CNTT hoặc các phương tiện thông tin đặt trong phòng máy chủ khiến hệ thống gặp lỗi vận hành; người làm việc trong phòng máy chủ có thể bị nhiễm điện qua nước ngập sàn.*



## 3.7 An toàn vật lý và môi trường<sup>(6)</sup>

---

### 3.7.3 Rủi ro (Risks)

➤ *Hệ quả (Consequences):*

- *Người phụ trách ATTT cho tài sản gặp rủi ro có thể phải bồi thường;*
- *Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền;*
- *Mục tiêu ngăn chặn truy cập vật lý trái phép, gây thiệt hại và can thiệp tới các phương tiện xử lý thông tin và thông tin của doanh nghiệp thất bại;*
- *Mục tiêu ngăn ngừa sự mất mát, hư hại, đánh cắp hoặc lợi dụng tài sản và làm gián đoạn hoạt động của doanh nghiệp thất bại.*

## 3.8 An toàn vận hành<sup>(1)</sup>

---

Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.12 có 7 Yêu cầu (A.12.1, A.12.2, A.12.3, A.12.4, A.12.5, A.12.6 và A.12.7) gồm 14 Điều (A.12.1.1,..., A.12.1.4, A.12.2.1, A.12.3.1, A.12.4.1,..., A.12.4.4, A.12.5.1, A.12.6.1, A.12.6.2 và A.12.7.1); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:

### 3.8.1 Điểm yếu được phát hiện:

- a) Không có văn bản quy định sao chép dữ liệu dự phòng ('Backup Data'); [A.12.1.1]
- b) Chưa trang bị đủ các máy chủ ứng dụng ('application server') và máy chủ dữ liệu ('database server') để phân tách các chức năng phát triển, kiểm thử và vận hành; [A.12.1.4]
- c) Không có máy tính nào được cài đặt phần mềm chống vi-rut máy tính. [A.12.2.1]

## 3.8 An toàn vận hành<sup>(2)</sup>

### 3.8.2 Mỗi đe dọa được nhận ra:

- a) Sao chép dự phòng thiếu hoặc không sao chép định kỳ;
- b) Sử dụng nhầm dữ liệu kiểm thử với dữ liệu thực hoặc kiểm thử sai môi trường khi kiểm thử phần mềm/ứng dụng;
- c) Mã độc (“malware”) như virus, worm, spyware, Adware, Trojan horse...tấn công



## 3.8 An toàn vận hành<sup>(3)</sup>

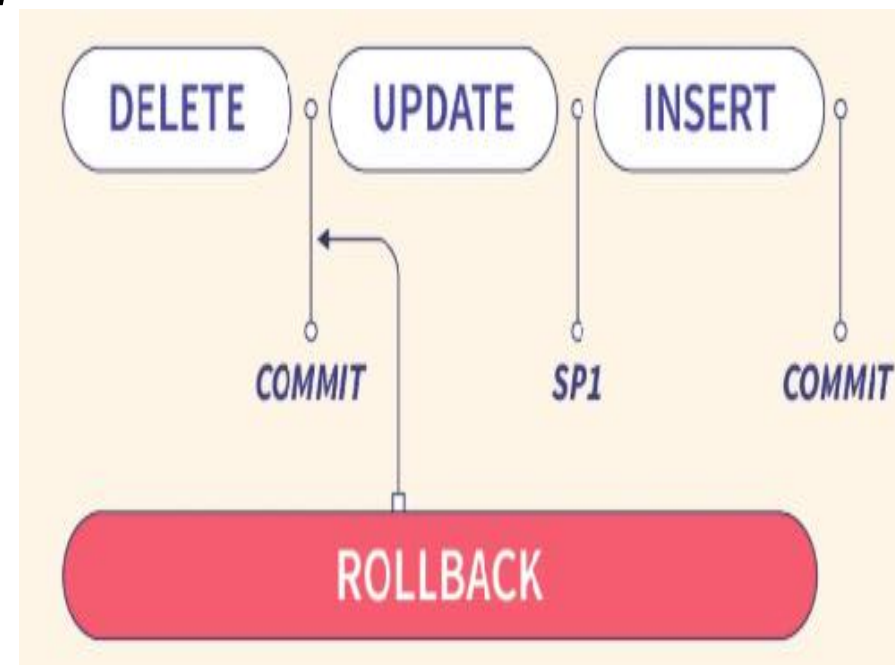
### 3.8.3 Rủi ro (Risks)

a) Người quản trị hệ thống có thể không có dữ liệu dự phòng khi cần phục hồi ('rollback');

b) Dữ liệu thực có thể bị thay đổi ngoài kiểm soát;

c) Máy tính có thể bị ngừng hoạt động do nhiễm mã độc (virus, worm, spyware, Adware, Trojan horse...).

➤ Khả năng xảy ra (Likelihood):  $< > 0\%$  / [tần suất]



## 3.8 An toàn vận hành<sup>(4)</sup>

---

### 3.8.3 Rủi ro (Risks)

➤ *Hệ quả (Consequences):*

- *Không thể phục hồi hệ thống (“system recovery”) bằng dữ liệu dự phòng nếu bị tấn công bởi “ransomware”;*
- *Làm hỏng dữ liệu thực trên hệ thống “production”; Người phụ trách ATTT cho hệ thống gặp rủi ro có thể bị kiện hoặc bị mất việc;*
- *Người dung máy tính không thể làm việc bình thường hoặc bị mất dữ liệu;*
- *Tài sản của doanh nghiệp bị tổn thất và có thể định lượng bằng tiền;*
- *Các mục tiêu ATTT khi vận hành hệ thống CNTT không đạt được.*

## 3.9 An toàn truyền thông<sup>(1)</sup>



## 3.9 An toàn truyền thông<sup>(2)</sup>

---

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.13 có 2 Yêu cầu (A.13.1 và A.13.2) gồm 7 Điều (A.13.1.1, A.13.1.2, A.13.1.3, A.13.2.1, A.13.2.2, A.13.2.3 và A.13.2.4); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### **3.9.1 Điểm yếu được phát hiện:**

*a) Dữ liệu trao đổi trên đường truyền giữa doanh nghiệp với các đơn vị khác bên ngoài chưa được bảo vệ bằng biện pháp mã hóa theo chính sách. [A.13.2.1]*

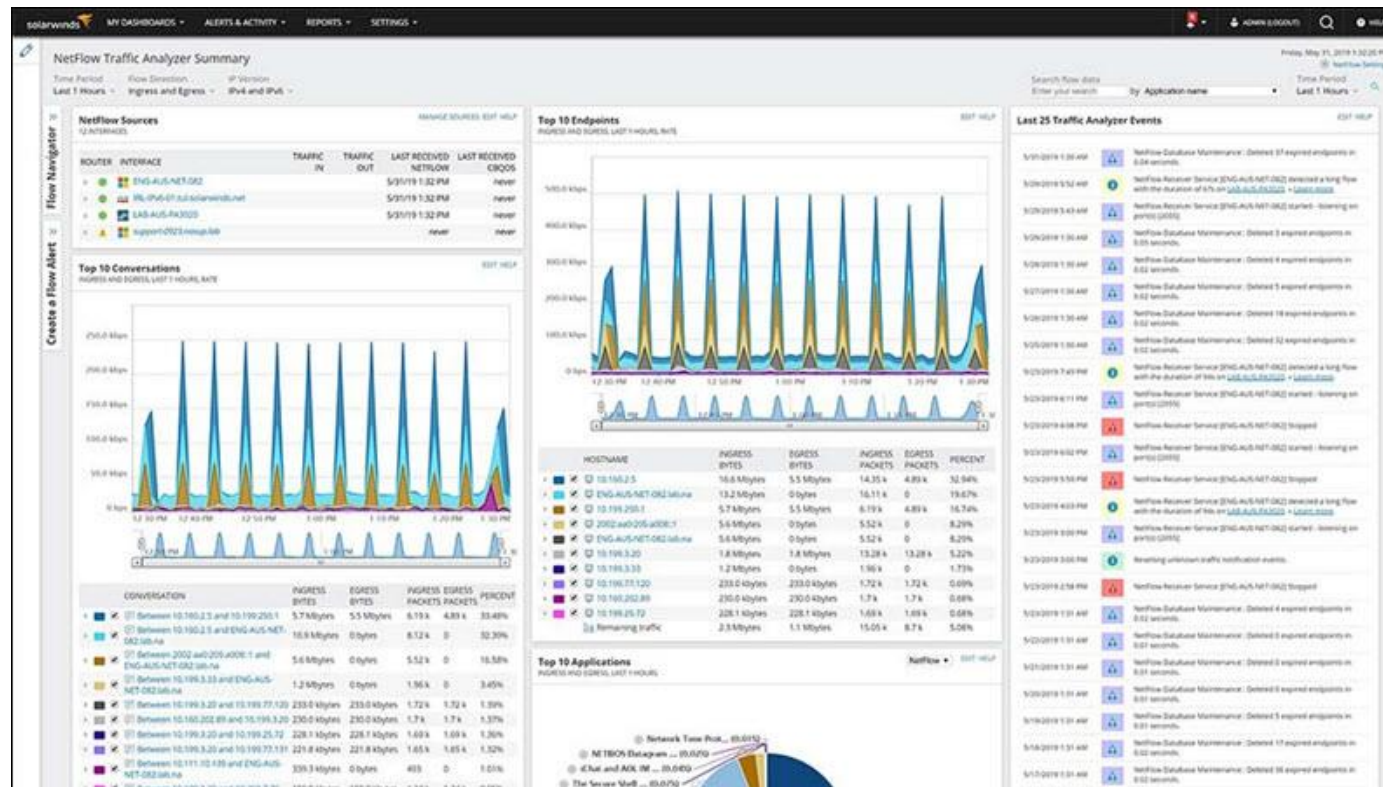
```
openssl enc -aes-256-cbc -salt -in input_file -out encrypted_file
```



## 3.9 An toàn truyền thông<sup>(3)</sup>

### 3.9.1 Điểm yếu được phát hiện:

b) Chưa sử dụng phần mềm (công cụ, tiện ích) theo dõi và giám sát hoạt động của hệ thống mạng ('Network Monitoring Tools'). [A.13.1.1]

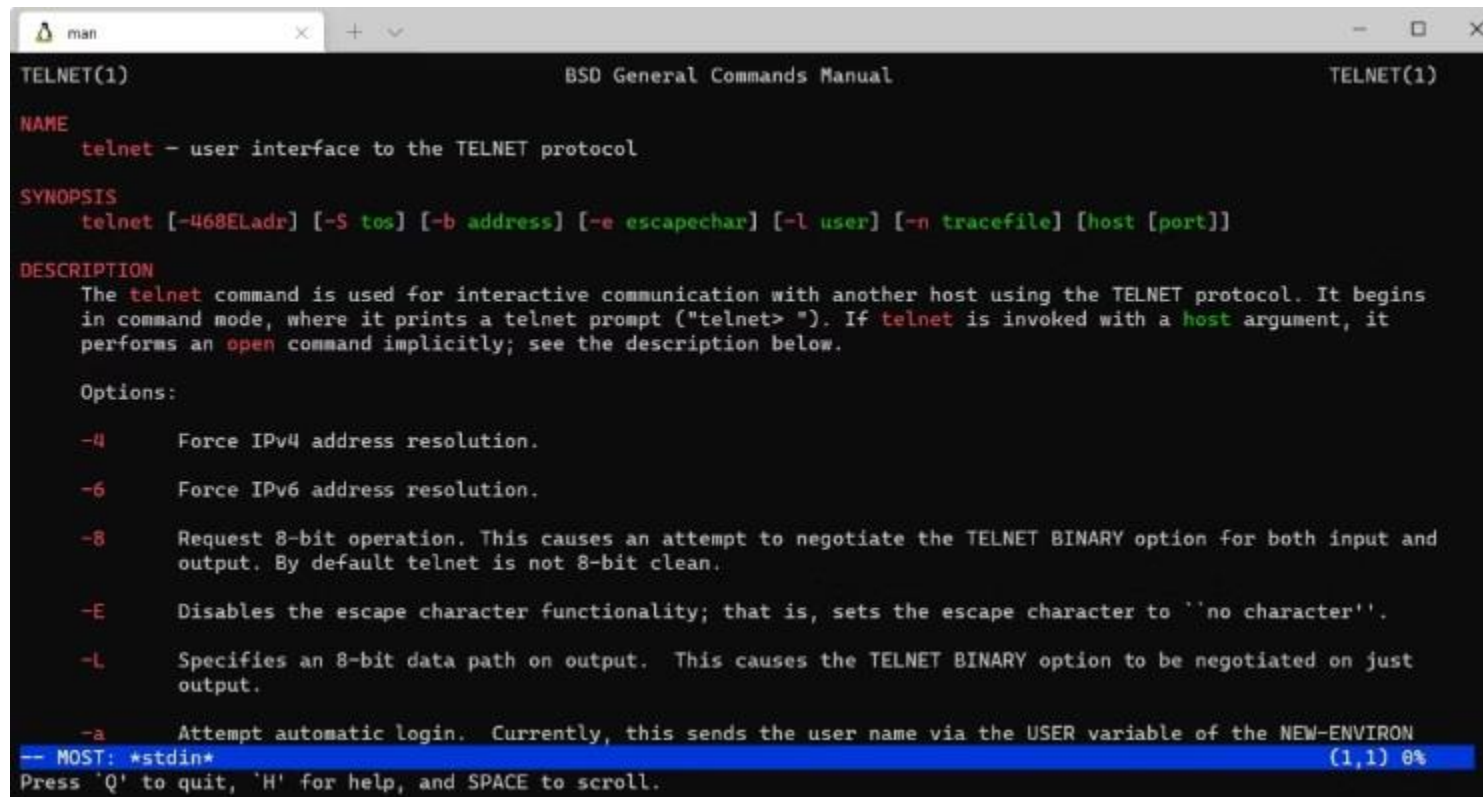




## 3.9 An toàn truyền thông<sup>(4)</sup>

### 3.9.1 Điểm yếu được phát hiện:

c) Dùng giao thức Telnet để thiết lập kết nối với một máy tính từ xa. [A.13.2.1]



```
man TELNET(1) BSD General Commands Manual TELNET(1)

NAME
telnet - user interface to the TELNET protocol

SYNOPSIS
telnet [-468ELadr] [-S tos] [-b address] [-e escapechar] [-l user] [-n tracefile] [host [port]]

DESCRIPTION
The telnet command is used for interactive communication with another host using the TELNET protocol. It begins
in command mode, where it prints a telnet prompt ("telnet> "). If telnet is invoked with a host argument, it
performs an open command implicitly; see the description below.

Options:
-4      Force IPv4 address resolution.
-6      Force IPv6 address resolution.
-8      Request 8-bit operation. This causes an attempt to negotiate the TELNET BINARY option for both input and
output. By default telnet is not 8-bit clean.
-E      Disables the escape character functionality; that is, sets the escape character to 'no character'.
-L      Specifies an 8-bit data path on output. This causes the TELNET BINARY option to be negotiated on just
output.
-a      Attempt automatic login. Currently, this sends the user name via the USER variable of the NEW-ENVIRON

-- MOST: *stdin* (1,1) 0%
Press 'Q' to quit, 'H' for help, and SPACE to scroll.
```

## 3.9 An toàn truyền thông<sup>(5)</sup>

---

### 3.9.2 Mỗi đe dọa được nhận ra:

- a) Vi phạm quy định bảo mật truyền dữ liệu (“Data in Motion”) theo chính sách ATTT của doanh nghiệp đã ban hành;*
- b) Truy cập mạng trái phép; tải dữ liệu tùy tiện không kiểm soát;*
- c) Dữ liệu truyền đi qua Telnet không an toàn.*

### 3.9.3 Rủi ro (Risks)

- a) Kẻ tấn công mạng (hay tội phạm mạng) hoặc kẻ xấu nội bộ có thể truy cập và đọc được dữ liệu của doanh nghiệp;*

## 3.9 An toàn truyền thông<sup>(6)</sup>

### 3.9.3 Rủi ro (Risks) (tiếp)

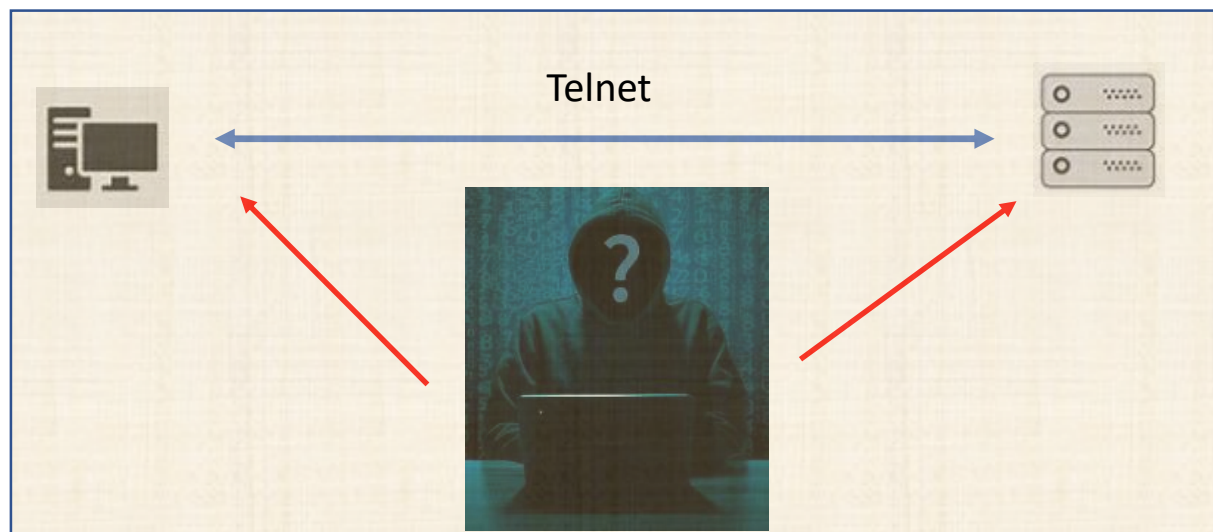
*b) Mạng có thể bị bão hòa lưu lượng mạng dẫn đến độ trễ cao, tốc độ chậm, mất gói tin...(do không phát hiện sớm hoạt động bất thường trên mạng như truyền tải dữ liệu (download/ upload), do không giám sát mạng).*

```
$ ping 50.X.X.X
PING 50.X.X.X (50.X.X.X) 56(84) bytes of data.
64 bytes from 50.X.X.X: icmp_seq=1 ttl=57 time=1135 ms
64 bytes from 50.X.X.X: icmp_seq=2 ttl=57 time=1106 ms
64 bytes from 50.X.X.X: icmp_seq=3 ttl=57 time=1161 ms
64 bytes from 50.X.X.X: icmp_seq=4 ttl=57 time=1115 ms
64 bytes from 50.X.X.X: icmp_seq=5 ttl=57 time=1096 ms
64 bytes from 50.X.X.X: icmp_seq=6 ttl=57 time=1108 ms
64 bytes from 50.X.X.X: icmp_seq=7 ttl=57 time=1144 ms
64 bytes from 50.X.X.X: icmp_seq=8 ttl=57 time=1131 ms
--- 50.X.X.X ping statistics ---
10 packets transmitted, 8 received, 20% packet loss, time 9118ms
```

## 3.9 An toàn truyền thông<sup>(6)</sup>

### 3.9.3 Rủi ro (Risks)

c) Người dùng có thể bị tấn công "man-in-the-middle attack" khi dùng Telnet.



- Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]
- Hệ quả (Consequences):
  - Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền;

## 3.9 An toàn truyền thông<sup>(7)</sup>

---

### 3.9.3 Rủi ro (Risks)

- *Thông tin tài khoản đăng nhập và/hoặc dữ liệu truyền đi bị kẻ tấn công chiếm đoạt, tính toàn vẹn thông tin bị mất (do bị kẻ tấn công sửa đổi);*
- *Lộ thông tin mật khiến khách hàng không tin tưởng dịch vụ của doanh nghiệp;*
- *Mạng bị chậm hoặc bị gián đoạn do độ trễ cao trên mạng và các vấn đề về hiệu suất mạng khi các gói tiếp theo bắt đầu vào đệm, cuối cùng là hết thời gian chờ và hiển thị các triệu chứng như tốc độ chậm và mất gói tin.*
- *Người phụ trách ATTT cho mạng bị mất việc khi hiệu suất mạng luôn bị giảm;*
- *Mục tiêu đảm bảo ATTT trong các mạng bị ảnh hưởng tiêu cực (hay thất bại).*

## 3.10 Tiếp nhận, phát triển và duy trì hệ thống<sup>(1)</sup>

Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.14 có 3 Yêu cầu (A.14.1, A.14.2 và A.14.3) gồm 13 Điều (A.14.1.1, A.14.1.2, A.14.1.3, A.14.2.1,..., A.14.2.9 và A.14.3.1); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:

### 3.10.1 Điểm yếu được phát hiện:

Chưa có thủ tục kiểm soát sự thay đổi hệ thống.  
[A.14.2.2]

### 3.10.2 Mối đe dọa được nhận ra:

Việc thay đổi vào hệ thống bị thất bại không nằm trong dự tính (chưa dự tính sẽ làm gì nếu thất bại).



## 3.10 Tiếp nhận, phát triển và duy trì hệ thống<sup>(2)</sup>

---

### 3.10.3 Rủi ro (Risks)

Lỗi có thể xảy ra (ngoài dự tính) khiến hệ thống không thể vận hành như trước đây sau khi đưa hệ thống vào sử dụng (khai thác).

- Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]
- Hệ quả (Consequences):
  - Gián đoạn chuỗi cung ứng dịch vụ cho khách hàng;
  - Người phụ trách ATTT cho hệ thống gặp rủi ro có thể bị mất việc;
  - Tài sản của doanh nghiệp bị tổn thất có thể định lượng bằng tiền;
  - Mục tiêu đảm bảo ATTT trong vòng đời phát triển bị thất bại.



## 3.11 Quan hệ với nhà cung cấp<sup>(1)</sup>

Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.15 có 2 Yêu cầu (A.15.1 và A.15.2) gồm 5 Điều (A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1 và A.15.2.2); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:

### 3.11.1 Điểm yếu được phát hiện:

Hợp đồng với nhà cung cấp không có nội dung thỏa thuận bảo mật thông tin (Non-Disclosure Agreement - NDA) với nhà cung cấp bằng văn bản. [A.15.1.1]

### 3.11.2 Mối đe dọa được nhận ra:

Sự lạm dụng quyền hạn (của nhà cung cấp) được cấp trên hệ thống được truy cập.





## 3.11 Quan hệ với nhà cung cấp<sup>(2)</sup>

---

### 3.11.3 Rủi ro (Risks)

*Nhà cung cấp có thể trộm cắp thông tin và tiết lộ thông tin cho các cá nhân hay tổ chức bên ngoài hoặc cho đối thủ cạnh tranh với doanh nghiệp.*

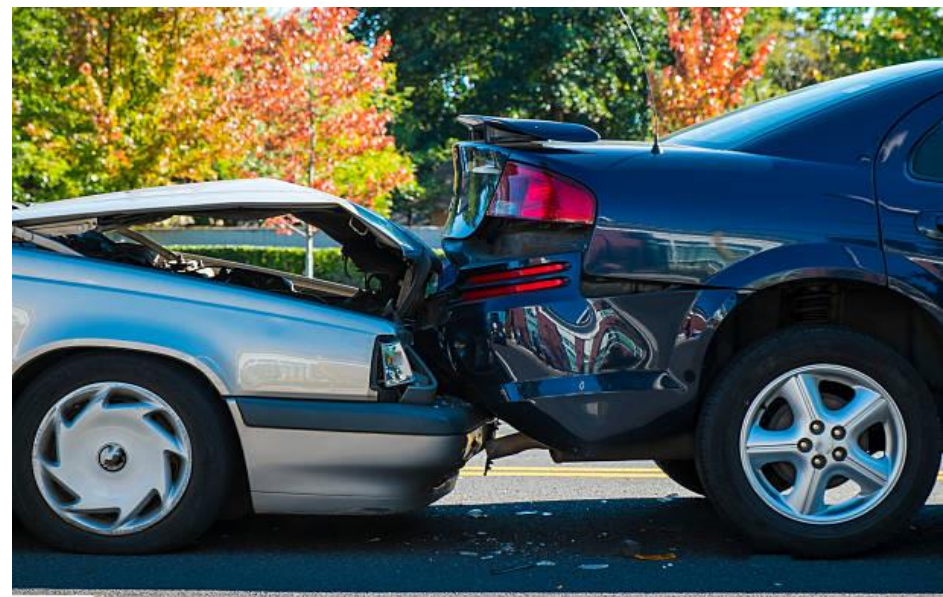
- *Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]*
- *Hệ quả (Consequences):*
  - *Không thể kiện nhà cung cấp vi phạm bảo mật thông tin;*
  - *Người đại diện có ký tên trong Hợp đồng không có NDA có thể bị mất việc;*
  - *Mục tiêu bảo vệ tài sản được truy cập bởi các nhà cung cấp thất bại;*
  - *Tài sản và uy tín của doanh nghiệp bị tổn thất và có thể định lượng bằng tiền.*

## 3.12 Quản lý sự cố ATTT<sup>(1)</sup>

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.16 có Yêu cầu (A.16.1) gồm 7 Điều (A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 và A.16.1.7); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### 3.12.1 Điểm yếu được phát hiện:

- a) Chưa có thủ tục hoặc kịch bản ứng phó với sự cố an toàn thông tin (ATTT);[A.16.1.5]*
- b) Chưa có quy trình xác định, tập hợp, thu thập và bảo quản thông tin có thể được dùng làm bằng chứng. [A.16.1.7]*



## 3.12 Quản lý sự cố ATTT<sup>(2)</sup>

---

### 3.12.2 Mối đe dọa được nhận ra:

- a) Kẻ tấn công có chủ đích (như APT) nhắm vào doanh nghiệp;*
- b) Hành động thu thập bằng chứng về sự cố không phù hợp.*



## 3.12 Quản lý sự cố ATTT<sup>(3)</sup>

---

### 3.12.3 Rủi ro (Risks)

a) Nhân viên gặp sự cố có thể không biết bắt đầu làm gì.[A.16.1.5]

b) Nhân viên sự cố không thu thập đủ bằng chứng về sự cố.[A.16.1.2].

➤ Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]

➤ Hệ quả (Consequences):

- Gián đoạn hoạt động kéo dài do không biết cách xử lý hoặc xử lý sai cách;
- Công tác điều tra và rút bài học kinh nghiệm hậu sự cố không đầy đủ;
- Tài sản và uy tín của doanh nghiệp bị tổn thất và định lượng được bằng tiền;
- Mục tiêu về cách tiếp cận hiệu quả, nhất quán với sự cố bị thất bại.

## 3.13 ATTT trong quản lý liên tục hoạt động<sup>(1)</sup>

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.17 có 2 Yêu cầu (A.17.1 và A.17.2) gồm 4 Điều (A.17.1.1, A.17.1.2, A.17.1.3 và A.17.2.1); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### 3.13.1 Điểm yếu được phát hiện:

*Không có thiết bị mạng (Router, Switch...) dự phòng tại doanh nghiệp. [A.17.2.1]*

### 3.13.2 Mối đe dọa được nhận ra:

*Vòng đời thiết bị mạng kết thúc sớm hơn dự báo;  
Vi phạm về bảo trì thiết bị xảy ra.*



## 3.13 ATTT trong quản lý liên tục hoạt động<sup>(2)</sup>

### 3.13.3 Rủi ro (Risks)

*Thiết bị mạng duy nhất có thể không làm việc / bị hỏng.*

- *Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]*
- *Hệ quả (Consequences):*
  - *Gián đoạn vận hành do không có thiết bị thay thế;*
  - *Người phụ trách ATTT cho hệ thống gặp rủi ro có thể bị mất việc;*
  - *Mục tiêu về tính liên tục và tính sẵn sàng của ATTT thất bại;*
  - *Tài sản của doanh nghiệp bị tổn thất và định lượng được bằng tiền.*



## 3.14 Sự tuân thủ<sup>(1)</sup>

---

*Căn cứ vào Phụ lục A - Bảng A.1 – Nhóm A.18 có 2 Yêu cầu (A.18.1 và A.18.2) gồm 8 Điều (A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5, A.18.2.1, A.18.2.2 và A.18.2.3); người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp có:*

### **3.14.1 Điểm yếu được phát hiện:**

- a) Sử dụng phần mềm xử lý ảnh không có bản quyền; [A.18.1.2]*
- b) Chưa thực hiện soát xét ATTT (ví dụ 3 tháng một lần, tuần đầu tiên tháng 03 hàng năm v.v.). [A.18.2.1] [A.18.2.3]*



## 3.14 Sự tuân thủ<sup>(2)</sup>

---

### 3.14.2 Mối đe dọa được nhận ra:

- a) *Vi phạm luật sở hữu trí tuệ và bản quyền.*
- b) *Vi phạm yêu cầu rà soát ATTT định kỳ.*





## 3.14 Sự tuân thủ<sup>(3)</sup>

### 3.14.3 Rủi ro (Risks)

- a) Doanh nghiệp có thể bị kiện ra tòa hoặc bị nhà cung cấp cảnh cáo do vi phạm quyền sở hữu trí tuệ và bản quyền phần mềm;
- b) Một số ứng dụng (phần mềm) có thể không được cập nhật/bảo trì/nâng cấp/vá lỗi.
- Khả năng xảy ra (Likelihood):  $<>0\%$  / [tần suất]



## 3.14 Sự tuân thủ<sup>(4)</sup>

---

### 3.14.3 Rủi ro (Risks)

➤ *Hệ quả (Consequences)*

- *Doanh nghiệp bị phạt tiền vì vi phạm pháp luật;*
- *Mất uy tín trong cộng đồng kinh doanh do vi phạm quy định ATTT;*
- *Mục tiêu tuân thủ và tránh vi phạm pháp luật thất bại;*
- *Mục tiêu đảm bảo ATTT phù hợp với chính sách và thủ tục của doanh nghiệp thất bại.*

# Tài liệu hỗ trợ triển khai ISO 27001:2013

---

## 1. ISO 27000:2018

Information technology — Security techniques — Information security management systems — Overview and vocabulary

## 2. ISO 27002:2013

Information technology — Security techniques — Code of practice for information security controls

## 3. ISO 27005:2008

Information technology — Security techniques — Information security risk management

## 4. ISO 27033-1:2015

Information technology — Security techniques — Network security (Part 1, 2, 3, 4, 5, 6, 7)

## 5. ISO 22301:2019

Security and resilience — Business continuity management systems — Requirements

## Hết Chương 02

**Cám ơn tất cả Anh/Chị đã theo dõi Chương này**

(\*) Một số hình minh họa được tải từ trang <https://www.pexels.com/>, <https://pixabay.com/>, <https://www.websentra.com>, <https://vneconomy.vn>, Microsoft Bing, <https://www.paulahannahlaw.com/> ...