TỔNG QUAN
AN TOÀN MẠNG MÁY TÍNH

09/01/2025

ThS.Nguyễn Duy
duyn@uit.edu.vn

Nội Dung

- Bảo mật thông tin là gì
- Những thách thức trong bảo mật thông tin
- Phân loại người tấn công
- Mô hình quản lý hệ thống IT của doanh nghiệp

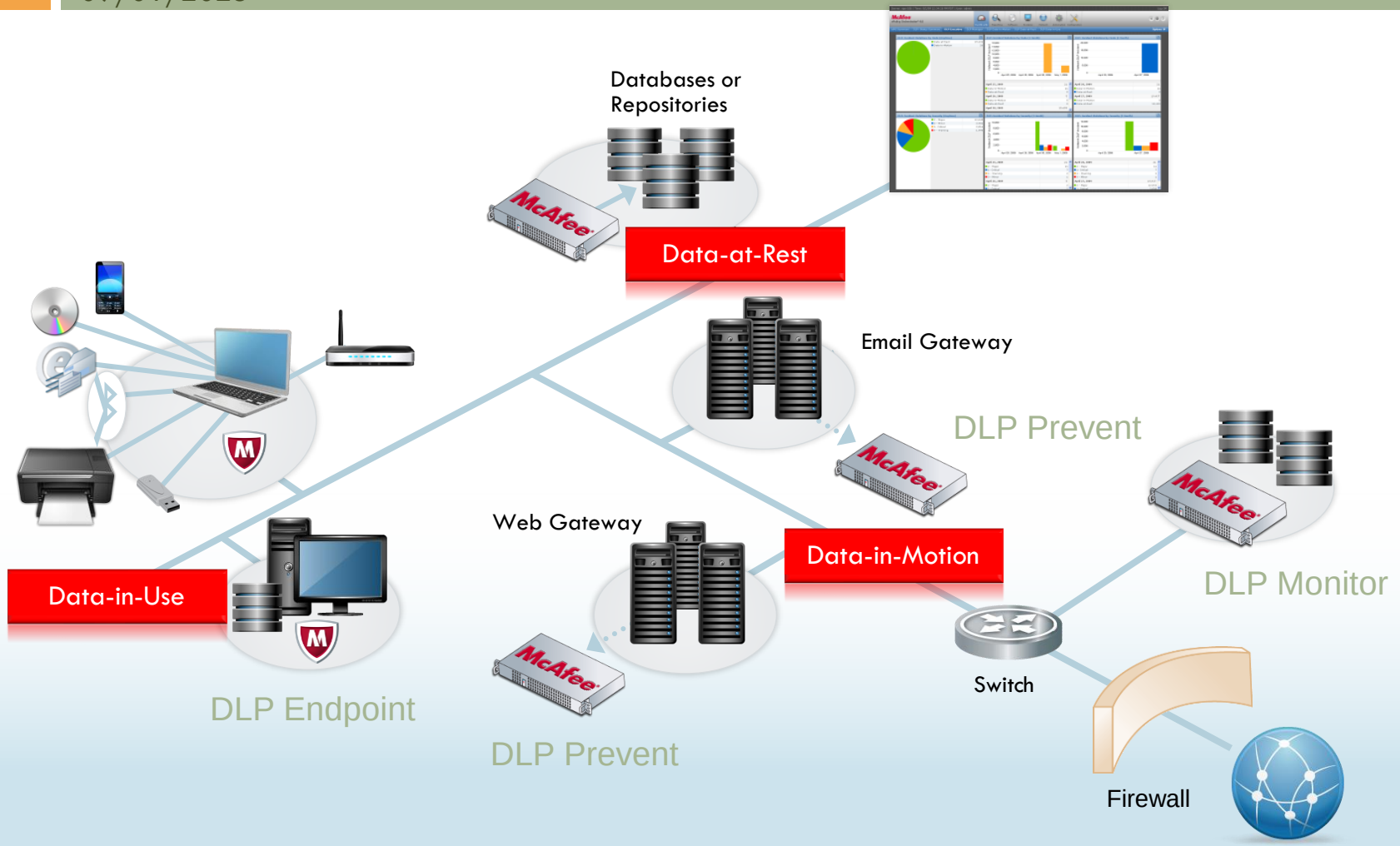
Nội Dung

- **Bảo mật thông tin là gì**
- Những thách thức trong bảo mật thông tin
- Phân loại người tấn công
- Mô hình quản lý hệ thống IT của doanh nghiệp

Bảo Mật Thông Tin Là Gì

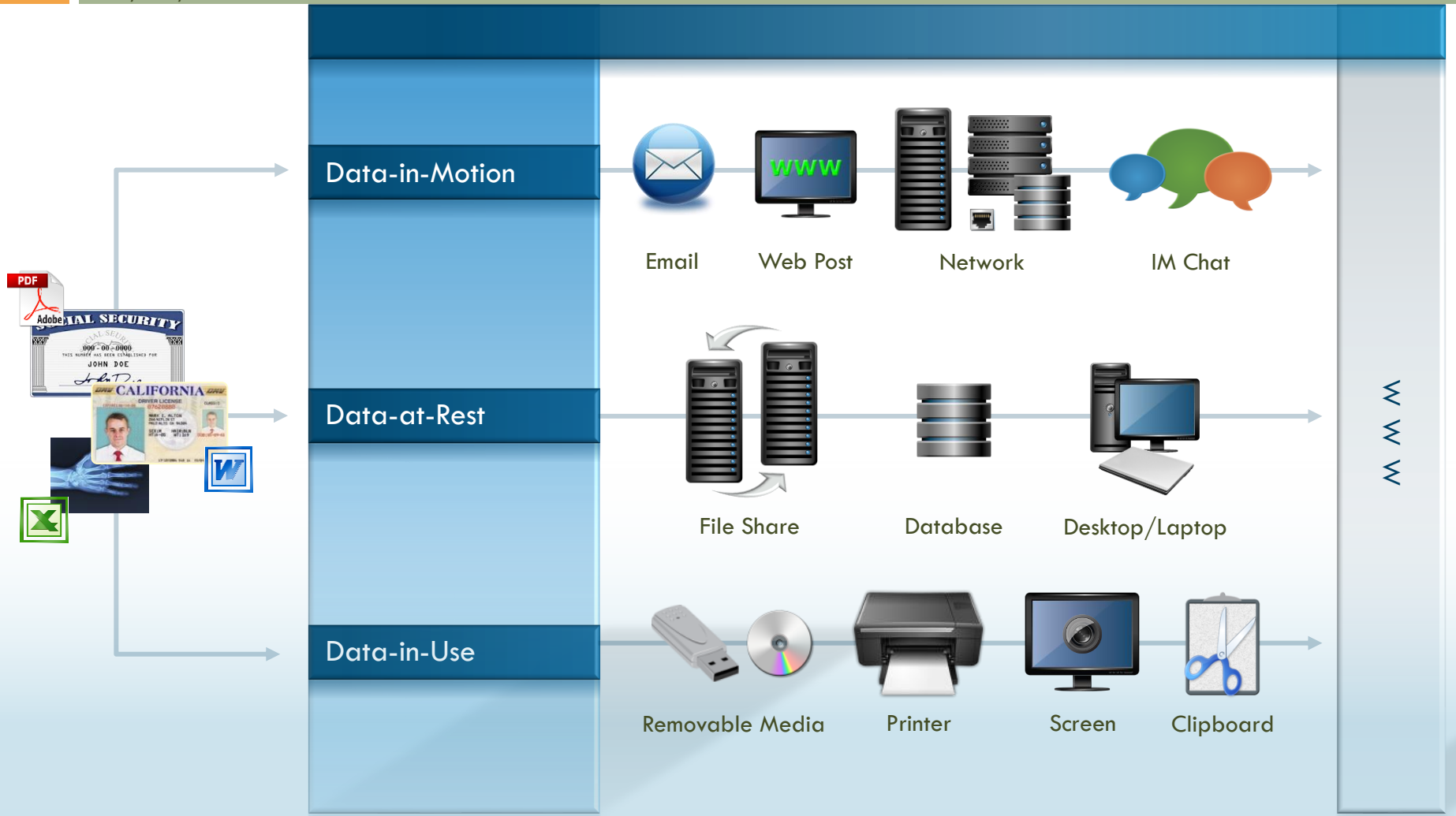
Những đặc điểm của thông tin

Bảo Mật Thông Tin Là Gì
Những trạng thái của thông tin



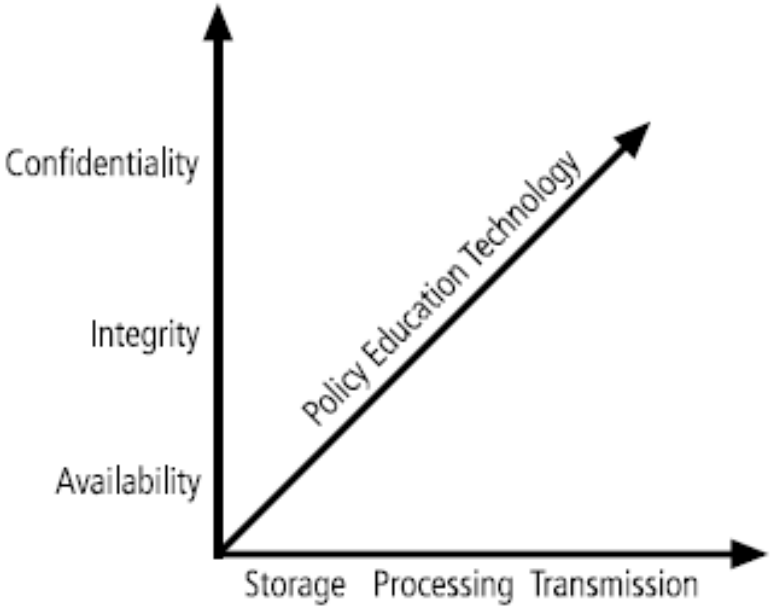
Bảo Mật Thông Tin Là Gì

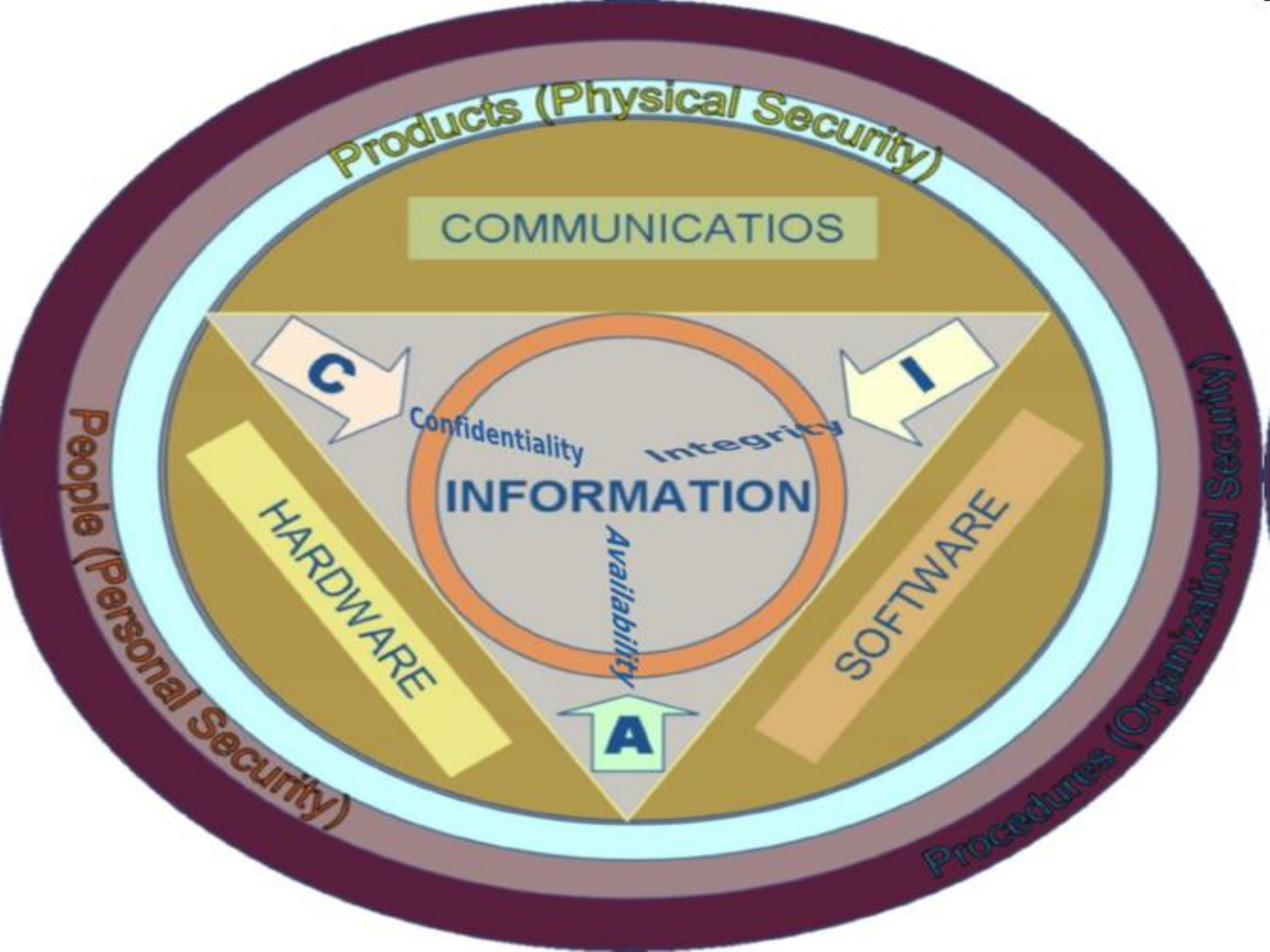
Những trạng thái của thông tin - tt



Bảo Mật Thông Tin Là Gì
Khái niệm

- Bảo mật thông tin là đảm bảo **tính bảo mật**, **tính toàn vẹn** và **tính sẵn sàng** của thông tin trên các thiết bị lưu trữ, trong quá trình sử dụng và truyền thông.




Products (Physical Security)
COMMUNICATIOS
C
I
Confidentiality
Integrity
INFORMATION
Availability
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

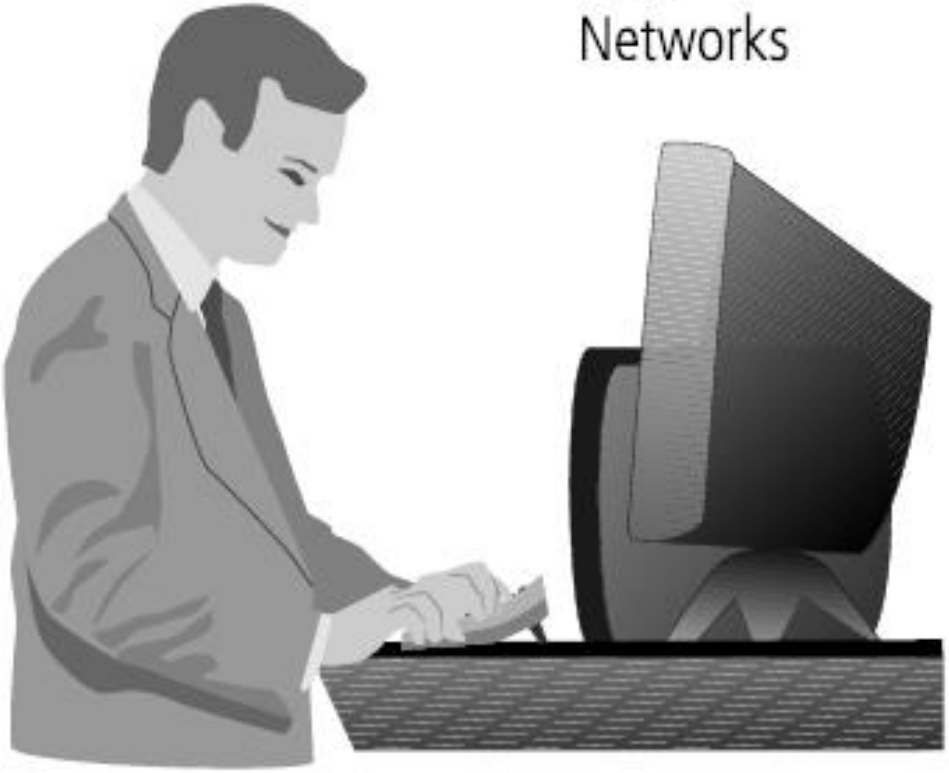
People

Hardware

Networks

Software

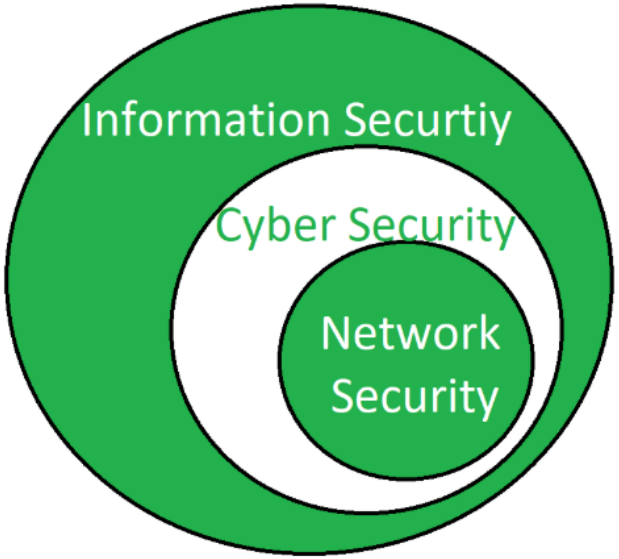
Procedures



Data

Information Security vs. Cyber Security vs. Network Security

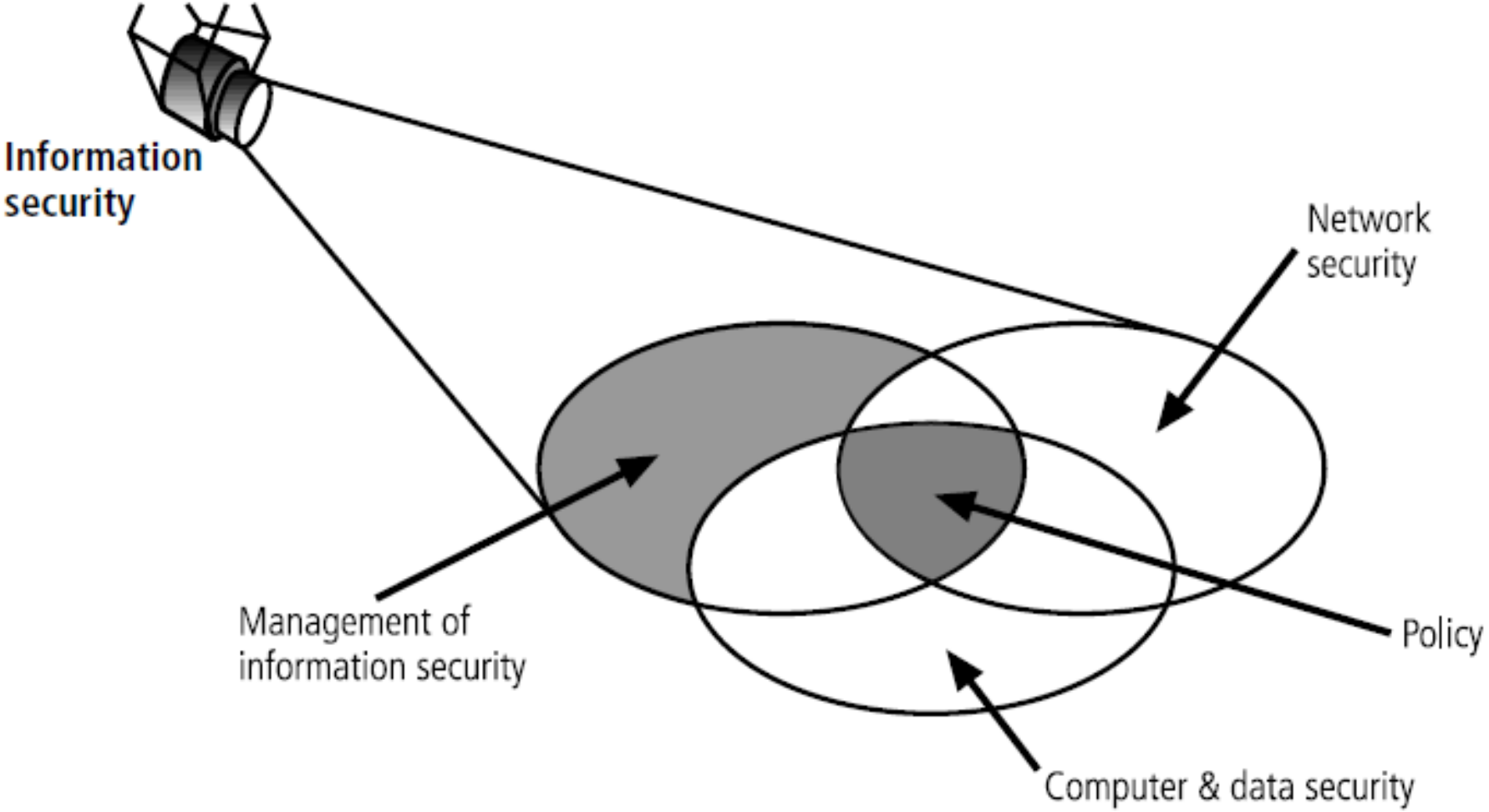
- **Cybersecurity (aka. Computer Security)**?
  - **<u>một nhánh của Information Security</u>**,
  - hoạt động bảo vệ mạng, máy tính và dữ liệu của tổ chức bạn khỏi truy cập kỹ thuật số trái phép, tấn công hoặc thiệt hại bằng cách triển khai nhiều quy trình, công nghệ và hoạt động khác nhau.
- **Network Security?**
  - **<u>một nhánh của Cyber Security,</u>**
  - nhằm bảo vệ mọi dữ liệu được gửi qua các thiết bị trong **mạng máy tính** để đảm bảo thông tin không bị thay đổi hoặc bị chặn.



Nội Dung

- Bảo mật thông tin là gì
- **Những thách thức trong bảo mật thông tin**
- Phân loại người tấn công
- Mô hình quản lý hệ thống IT của doanh nghiệp

Những Thách Thức Trong Bảo Mật Thông Tin



Những Thách Thức Trong Bảo Mật Thông Tin - tt

- Tính sẵn sàng của dữ liệu
  - Tấn công Denial of Service (DoS)
  - Tấn công Distributed Denial of Service (DDos)
  - Hệ thống ngưng hoạt động (System fail)
  - Rớt mạng (Network fail)
  - Cấu trúc dữ liệu bị phá hủy (malicious)

Những Thách Thức Trong Bảo Mật Thông Tin - tt

- Tính toàn vẹn của dữ liệu
  - Man in the middle
  - SQL Injection
  - Buffer Overload
  - Malicious code
  - Employee
  - Thuật toán bảo vệ tính toàn vẹn yếu

Những Thách Thức Trong Bảo Mật Thông Tin - tt

- Cập nhật toàn cầu về lực lượng lao động an ninh mạng năm 2020

Nghiên cứu toàn cầu của ISACA cho thấy việc tuyển dụng và giữ chân nhân viên an ninh mạng ngày càng khó khăn hơn

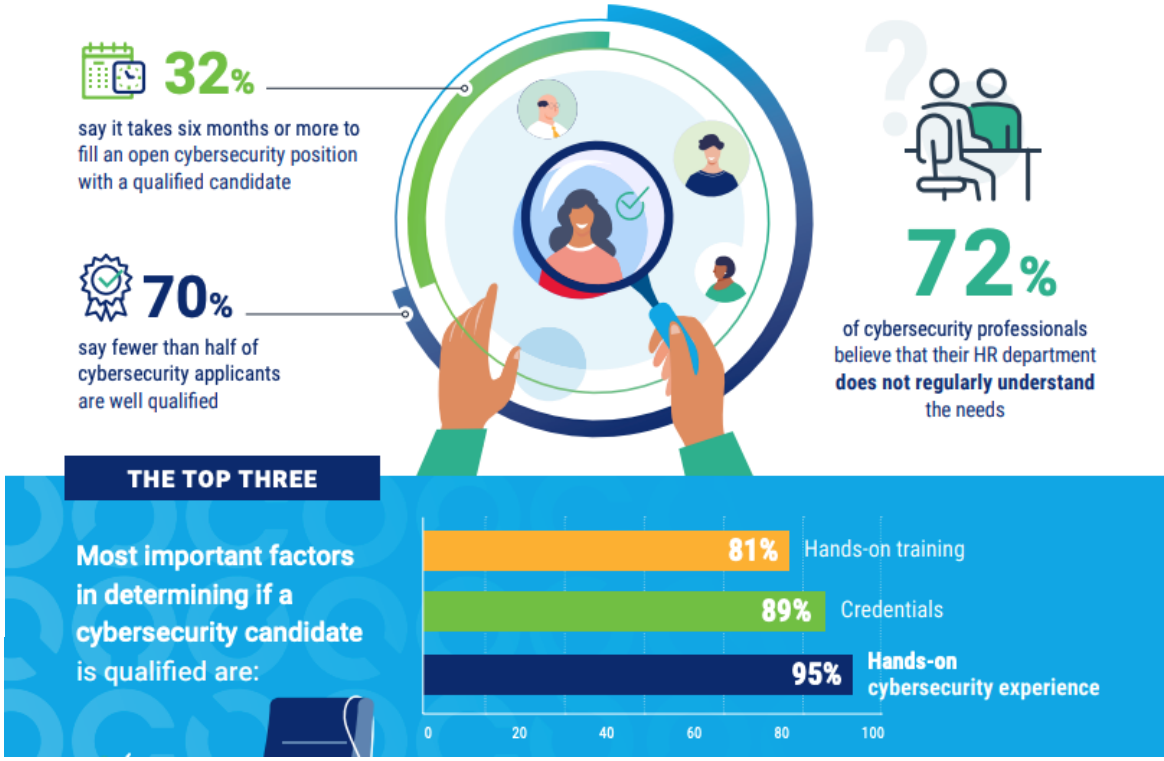
62%

say their organization's cybersecurity team is **understaffed**

57%

say they currently have **unfilled** cybersecurity positions on their team

* 2,051 respondents worldwide



Những Thách Thức Trong Bảo Mật Thông Tin – tt

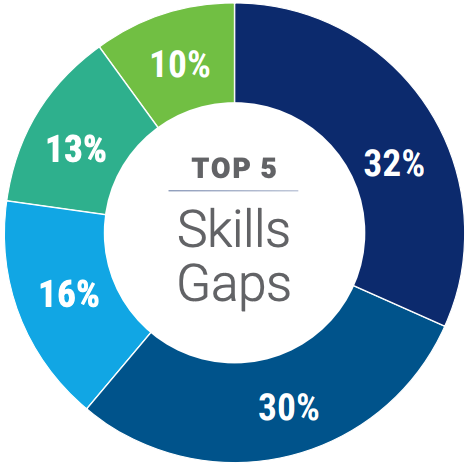
- Retention Concerns Increase & Skills Gaps Persist

TOP 5 REASONS

Respondents say cybersecurity staff are leaving:

1. **59%** Recruited by other companies
2. **50%** Limited promotion and development opportunities
2. **50%** Poor financial incentives
3. **40%** High work stress levels
4. **39%** Lack of management support

66% say it's **difficult** to retain cybersecurity talent (an increase from last year)



- Soft skills
- IT knowledge and skills gaps
- Insufficient business insight
- Cybersecurity technical experience
- Insufficient hands-on training

ONLY 27% say recent university graduates in cybersecurity **are well-prepared** for the cybersecurity challenges they'll face

81% of respondents say men and women are offered **equal opportunities** for career advancements at their organization

Những Thách Thức Trong Bảo Mật Thông Tin – tt

- Bối cảnh đe dọa và thực hành bảo mật

Giữa đại dịch COVID-19 - trong đó 92% chuyên gia kiểm toán và bảo mật CNTT cho biết **tội phạm mạng đang gia tăng**

MOST FREQUENT

Attack Methods

1. **Social engineering** (15%)
2. **Advanced persistent threat** (10%)
3. **Ransomware and unpatched systems** (9% each)

1. **22%** Cybercriminals
2. **19%** Hackers
3. **11%** Malicious insiders
4. **10%** Nonmalicious insiders
5. **9%** Nation-state attackers
6. **8%** Hacktivists

Nội Dung

- Bảo mật thông tin là gì
- Những thách thức trong bảo mật thông tin
- Phân loại người tấn công
- Mô hình quản lý hệ thống IT của doanh nghiệp

Nội Dung

- Bảo mật thông tin là gì
- Những thách thức trong bảo mật thông tin
- **Phân loại người tấn công**
- Mô hình quản lý hệ thống IT của doanh nghiệp

Phân Loại Người Tấn Công

- Black-hat hackers
- Script kiddies
- Cyber spies
- Vicious employees
- Cyber terrorists

Phân Loại Người Tấn Công
Black-hat hackers

- Hackers là những người có tri thức đặc biệt về hệ thống máy tính. Họ quan tâm đến những chi tiết tinh tế của phần mềm, giải thuật, mạng máy tính và cấu hình hệ thống. Họ là một nhóm người ưu tú, năng động, được đào tạo tốt.
- Tùy theo mục đích, hackers được chia thành hackers mũ đen, hackers mũ trắng và hackers mũ xám

- Black Hat hackers (crackers) → **cybercrime**
- White Hat hackers (ethical hackers)
- Gray Hat hackers

Phân Loại Người Tấn Công
Black-hat hackers

Top notorious cyber attacks in history

- 1988: **Morris Worm** – the first Internet worm
- 1994: Mitnick attack
- 2000: MafiaBoy attack
- 2008: Kaminsky attack

…

- 2014: Heartbleed attack
- 2016: Mirai Botnet: The fall of the Internet
- 2017: WannaCry: A real epidemic
- …

Top 10 Black-Hat Hackers in the World

Phân Loại Người Tấn Công

Script kiddies

- Là những người sử dụng các script hoặc các chương trình được phát triển bởi các hacker mũ đen (những công cụ hack) để tấn công các máy tính và gây thiệt hại cho người khác.
- Script kiddies chỉ biết sử dụng công cụ hack để tấn công các mục tiêu chứ không hiểu cách thức hoạt động và cũng không có khả năng viết ra những công cụ tương tự.
- Đa số Script kiddies chỉ là những thanh thiếu niên, không đủ nhận thức và chín chắn để hiểu hết những hậu quả do mình gây ra.

Phân Loại Người Tấn Công

Script kiddies

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES LECTURES

Business ▸ Policy

Bedroom NASA hacker set to bite pillow in choky

Pinecrest boy pining for freedom

By Linda Harrison 22 Sep 2000 at 14:52 SHARE ▼

A Florida teenager was banged up for six months yesterday after admitting he hacked into NASA systems.

Jonathan James, known as "cOmrade" on the Net, pleaded guilty to intercepting 3,300 emails, stealing passwords, and nicking data from 13 NASA computers - including some involved with the International Space Station.

The not-so-sweet 16-year-old will do time in a Florida detention centre - he was just 15 when the crimes occurred.

"Breaking into someone else's property, whether it's a robbery or a computer intrusion, is a serious crime," said Attorney General Janet Reno, *AP reported*

According to the *Miami Herald*, the lad sat in his bedroom in Pinecrest, Southern Florida, and used his Gateway Pentium 266 computer to access some of the world's most top-secret information.

He was busted by federal agents from Fort Lauderdale touting weapons and bulletproof vests. But not before he had downloaded $1.7 million in NASA proprietary software that supports its environmental systems. Apparently it

CPO MAGAZINE

HOME NEWS INSIGHTS RESOURCES

Share Tweet Share Pin it

The good news about the Twitter hack is that it does not appear to have been orchestrated by a nation-state group. The bad news is that it appears a bunch of relatively unsophisticated teenagers managed to get access to the communications channels of some of the most powerful people on Earth. The apparent ringleader is a Florida 17-year-old with a history of running small-time scams in Minecraft and who had previously been investigated for theft of bitcoin.

HACKERS

The Kid Who Hacked NASA Servers at Age 13 Now Has His Own Television Show

Add to Queue NEXT ARTICLE

Walter O'Brien, Founder & CEO, Scorpion Computer Services

Phân Loại Người Tấn Công
Cyber spies

- Có thể hoạt động trên lãnh vực quân sự, kinh tế,…
- Đánh chặn truyền thông trên mạng và phá mã các thông điệp đã được mã hoá.
- Nhiều tổ chức tình báo lớn trên thế giới đã thuê các nhà toán học, các nhà khoa học máy tính, các giáo sư đại học làm việc cho họ để phát triển các công cụ nhằm chống lại loại tội phạm này

Phân Loại Người Tấn Công

Cyber spies

Ashley Pugh | Cyber Security
Jun '18

How Stuxnet almost started World War III

There have been multiple occasions since World War II ended in 1945 that the world thought it would be engulfed in another global conflict: the 1979 NORAD computer glitch, the Cold War, the Cuban Missile Crisis (my history GCSE means I can tell you a lot about those), and the Black Brant scare to name a few.

The Stuxnet computer worm is another such incident, and probably won't be the last now that Donald Trump likes to play games of "my weapons are bigger than yours", which I have no doubt they are.

Stuxnet was a malicious software that targeted control systems in the Natanz nuclear facility in Iran. It enters a computer connected to the system through an infected removable hard-drive, expected to be a USB stick, then the worm uploaded itself onto the plant's computer system. It is still not known if Stuxnet was uploaded accidentally or deliberately. If done deliberately, it would have been the work of a double agent.

WIRED Hackers Take Down the Most Wired Country in Europe

HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were all down. The former director of the University of Tartu Institute of Experimental Physics and Technology had been the Estonian defense minister for only four weeks. He hadn't even changed the art on the walls.

An aide rushed in with a report. It wasn't just the newspapers. The leading bank was under siege. Government communications were going down. An enemy had invaded and was assaulting dozens of targets.

Outside, everything was quiet. The border guards had reported no incursions, and Estonian airspace had not been violated. The aide explained what was going on: They were under attack by a rogue computer network.

Phân Loại Người Tấn Công
Vicious employees

- Là những người cố tình vi phạm an ninh để làm hại những người sử dụng họ.
- Tấn công máy tính công ty để kiếm sự quan tâm từ những người lãnh đạo.
- Hoạt động như gián điệp mạng để thu thập và bán bí mật của công ty.

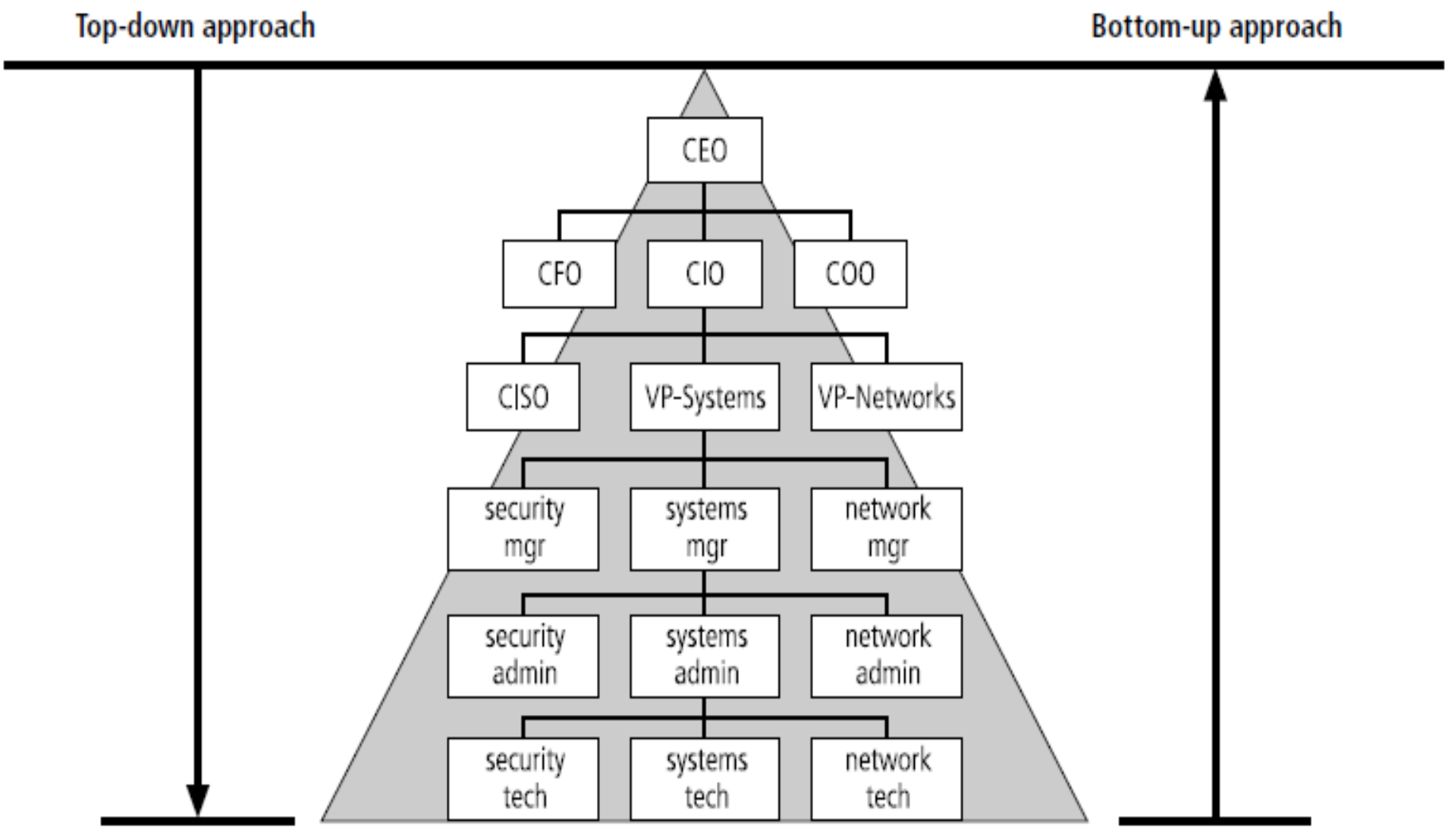
Phân Loại Người Tấn Công
Cyber terrorists

- Sử dụng có chủ đích các hoạt động phá hoại, hoặc đe dọa sử dụng các hoạt động đó, đối với máy tính và/hoặc mạng
- Mục đích gây hại hoặc thúc đẩy các mục tiêu xã hội, tư tưởng, tôn giáo, chính trị hoặc các mục tiêu tương tự, hoặc để đe dọa bất kỳ người nào nhằm thúc đẩy các mục tiêu đó.

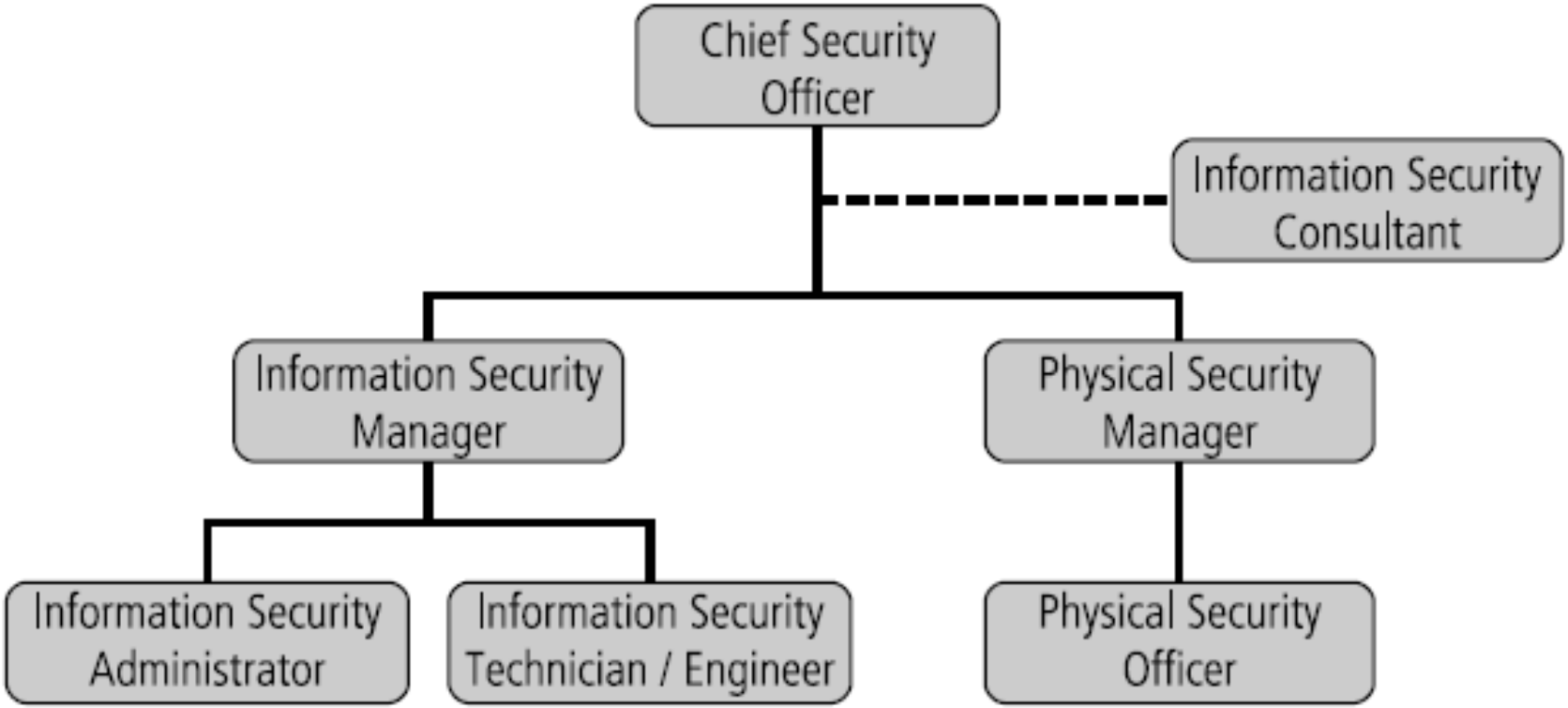
Nội Dung

- Bảo mật thông tin là gì
- Những thách thức trong bảo mật thông tin
- Phân loại người tấn công
- **Mô hình quản lý hệ thống IT của doanh nghiệp**

MÔ HÌNH QUẢN LÝ HỆ THỐNG IT TRONG DOANH NGHIỆP



MÔ HÌNH QUẢN LÝ HỆ THỐNG IT TRONG DOANH NGHIỆP



Question ???