AN TOÀN MẠNG MÁY TÍNH

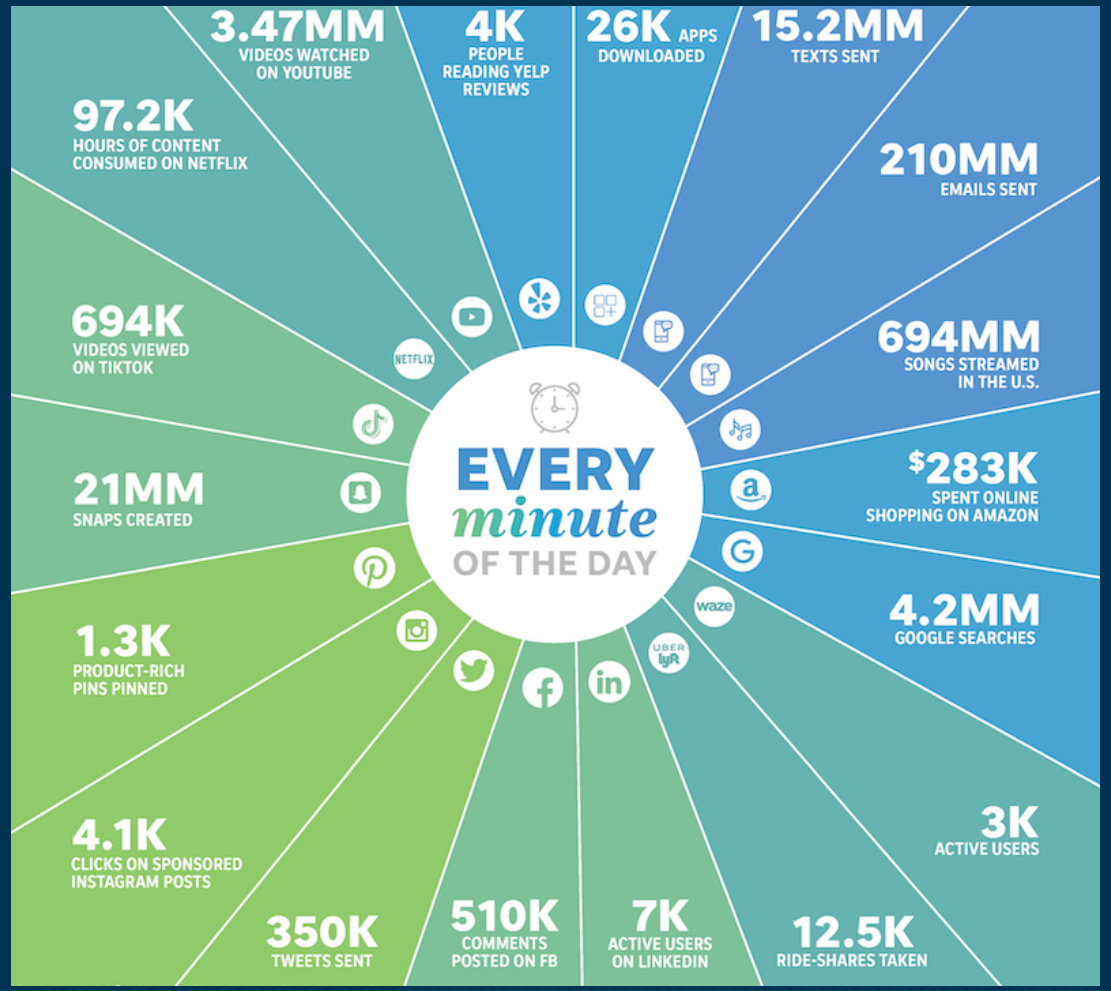
#01_TỔNG QUAN

ThS. Lê Đức Thịnh, UIT

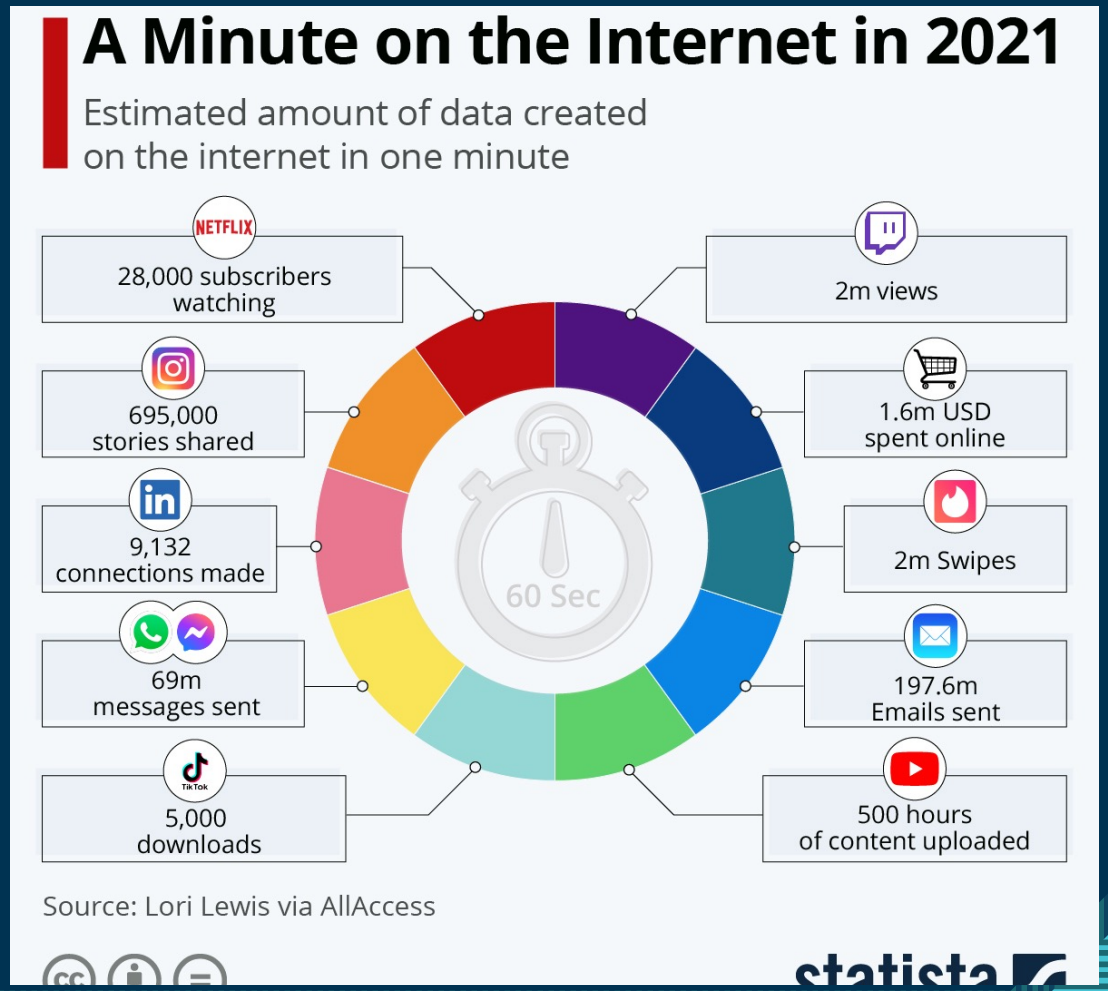
Nội dung

- An toàn thông tin và các vấn đề liên quan?
- Các Luật về an toàn, an ninh thông tin ở Việt Nam?
- Mô hình bảo mật
- Khuôn khổ an ninh (security framework)
- Quản lý rủi ro (risk management)

Một số thống kê



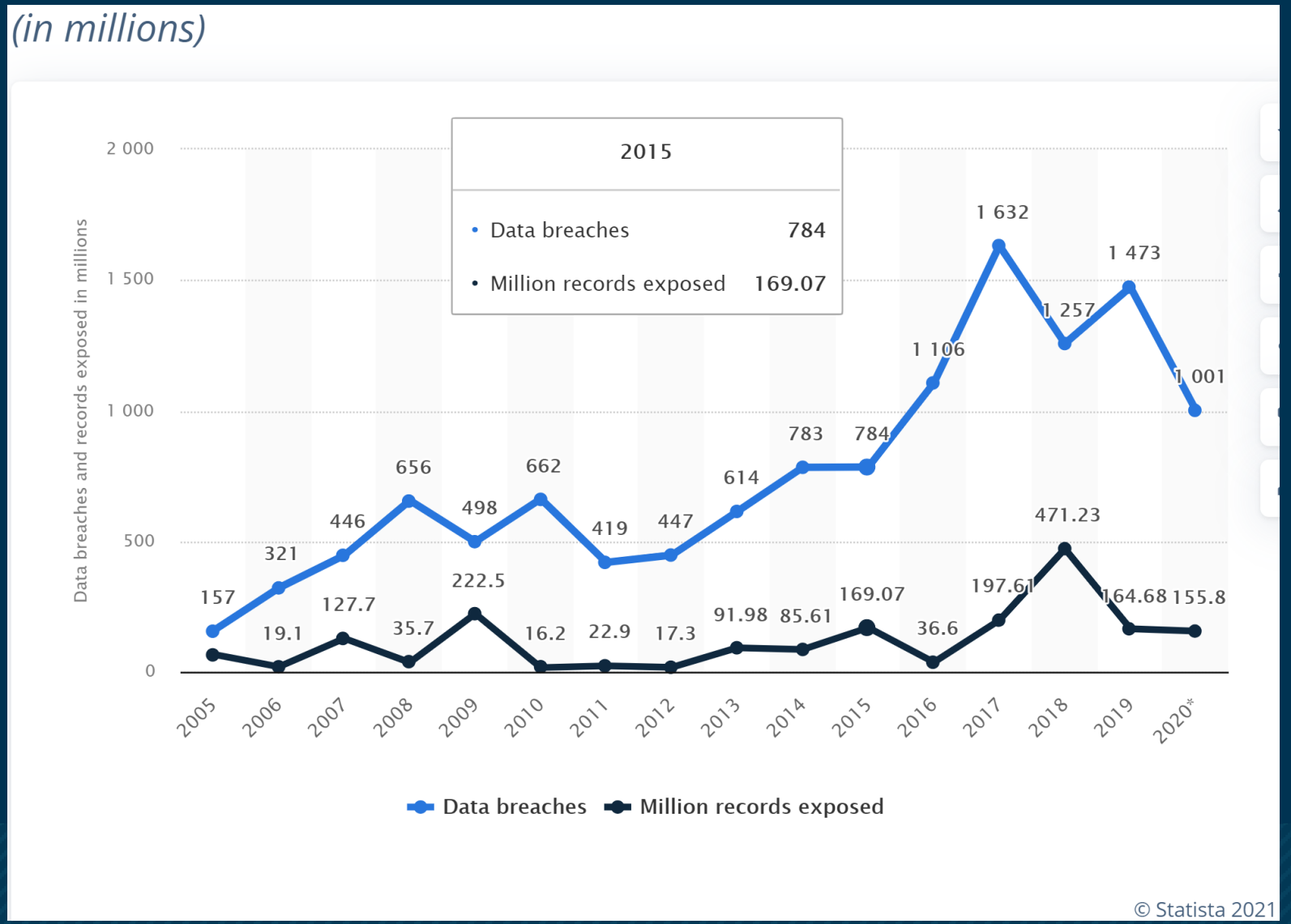
https://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/



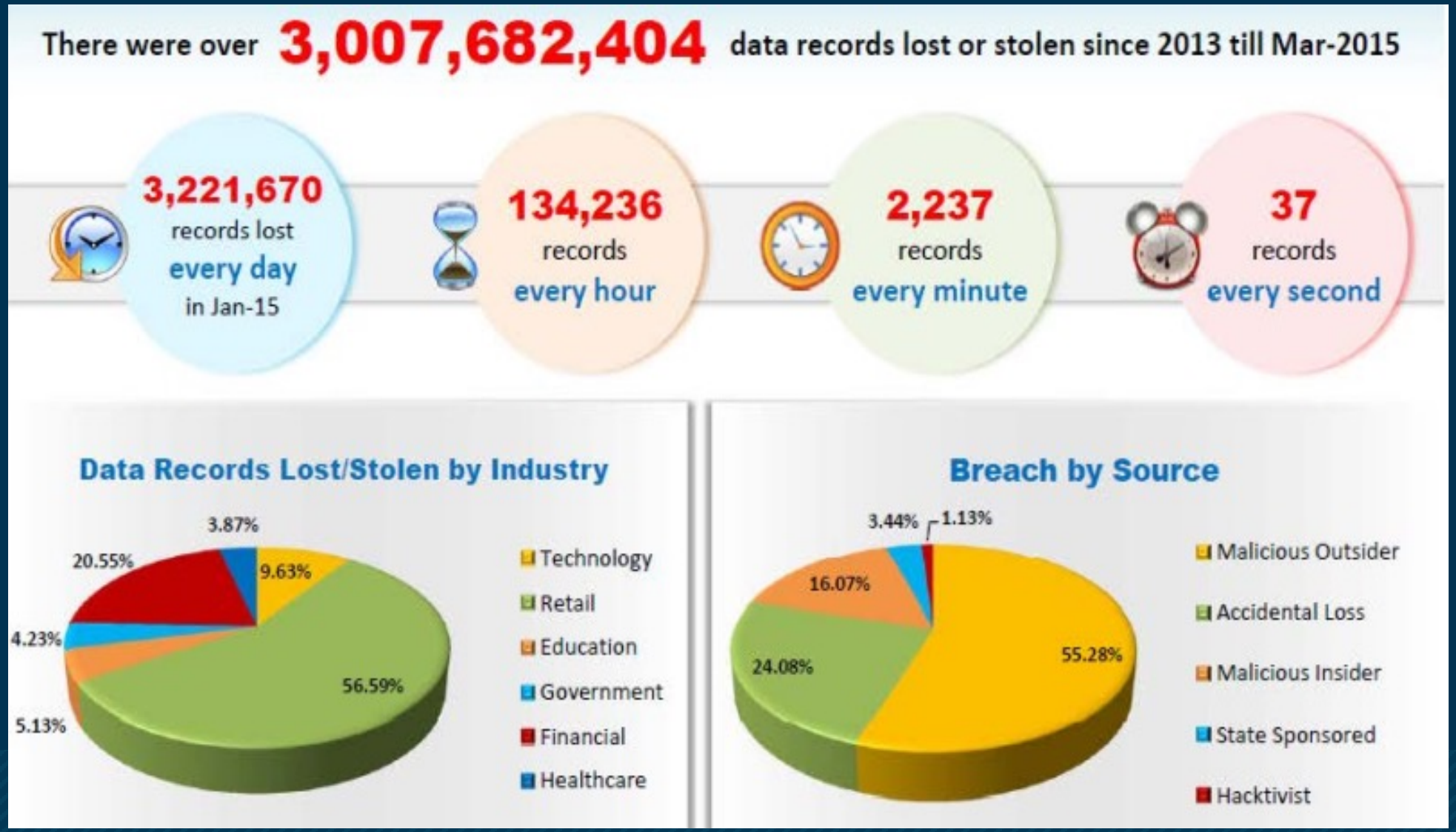
https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/

Một số thống kê

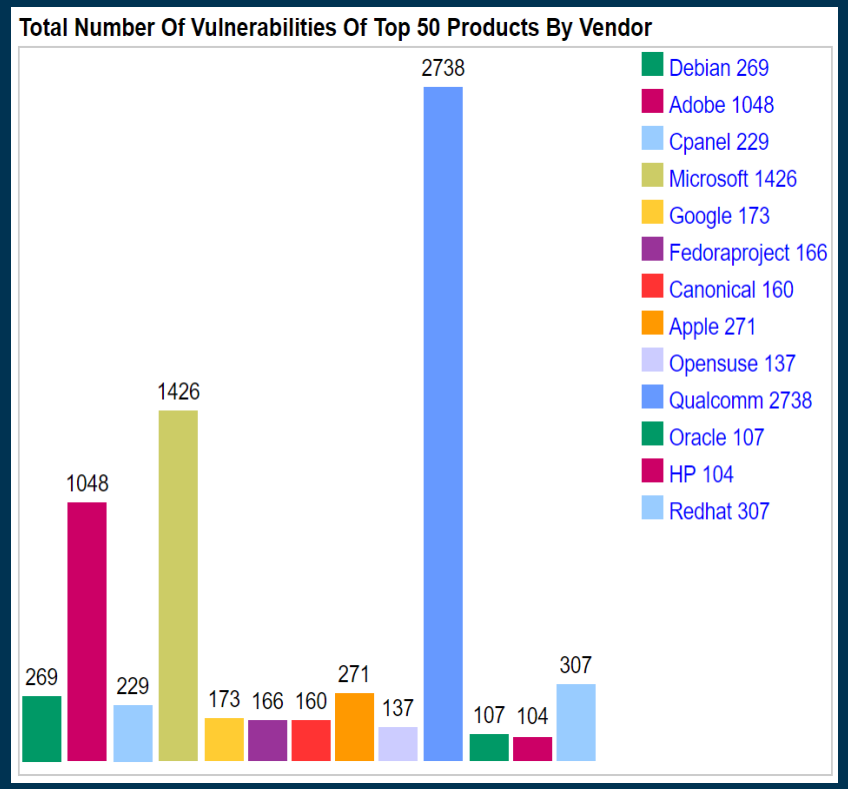
(in millions)



Một số thống kê



Một số thống kê Lỗi phần mềm



Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019

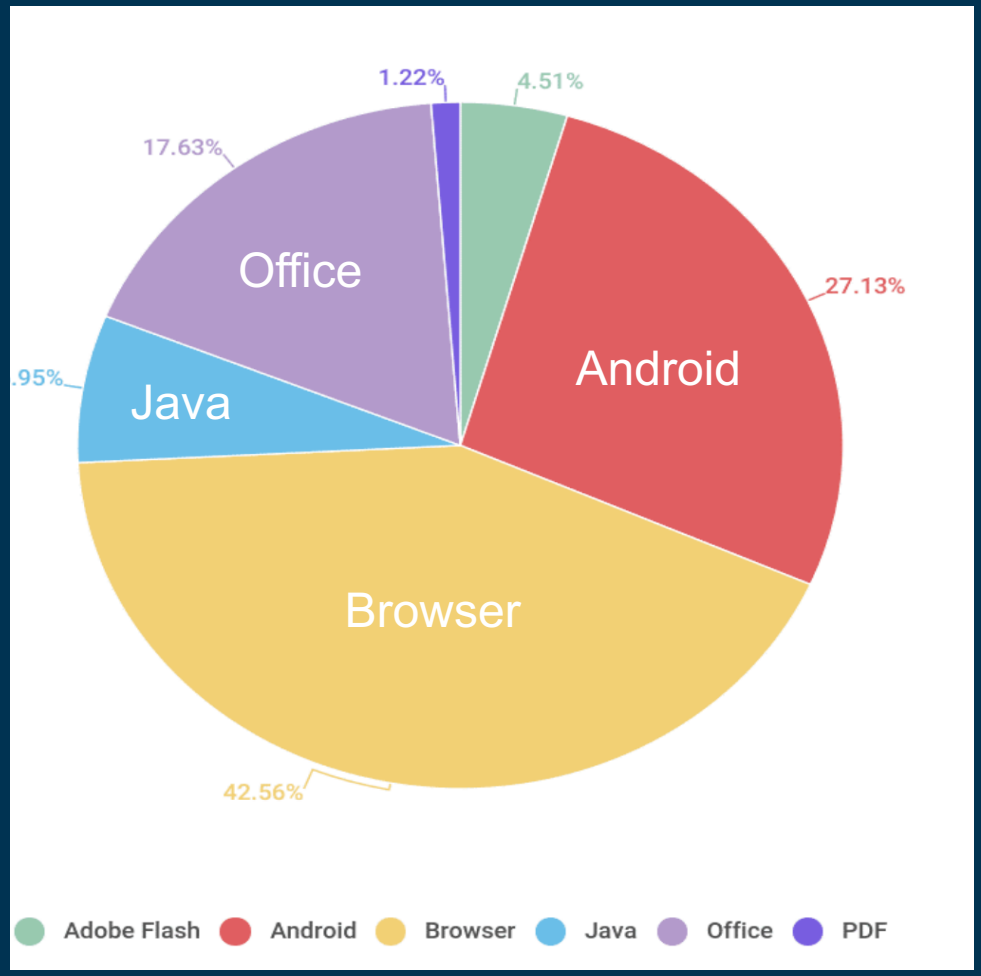
Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	269
2	Acrobat Reader	Adobe	Application	262
3	Acrobat	Adobe	Application	262
4	Acrobat Reader Dc	Adobe	Application	262
5	Acrobat Dc	Adobe	Application	262
6	Cpanel	Cpanel	Application	229
7	Windows Server 2016	Microsoft	OS	219
8	Windows 10	Microsoft	OS	218
9	Windows Server 2019	Microsoft	OS	217
10	Chrome	Google	Application	173
11	Fedora	Fedoraproject	OS	166
12	Ubuntu Linux	Canonical	OS	160
13	Windows 7	Microsoft	OS	158
14	Windows Server 2008	Microsoft	OS	158
15	Windows Server 2012	Microsoft	OS	156
16	Iphone Os	Apple	OS	155
17	Windows 8.1	Microsoft	OS	151
18	Windows Rt 8.1	Microsoft	OS	149
19	Leap	Opensuse	OS	137
20	Sd 625 Firmware	Qualcomm	OS	127
21	Mdm9607 Firmware	Qualcomm	OS	126
22	Sd 835 Firmware	Qualcomm	OS	119
23	Mdm9650 Firmware	Qualcomm	OS	119
24	Sdm660 Firmware	Qualcomm	OS	118
25	Sd 425 Firmware	Qualcomm	OS	117
26	Mdm9206 Firmware	Qualcomm	OS	116
27	Mac Os X	Apple	OS	116
28	Sd 636 Firmware	Qualcomm	OS	115

https://www.cvedetails.com/top-50-products.php?year=2019

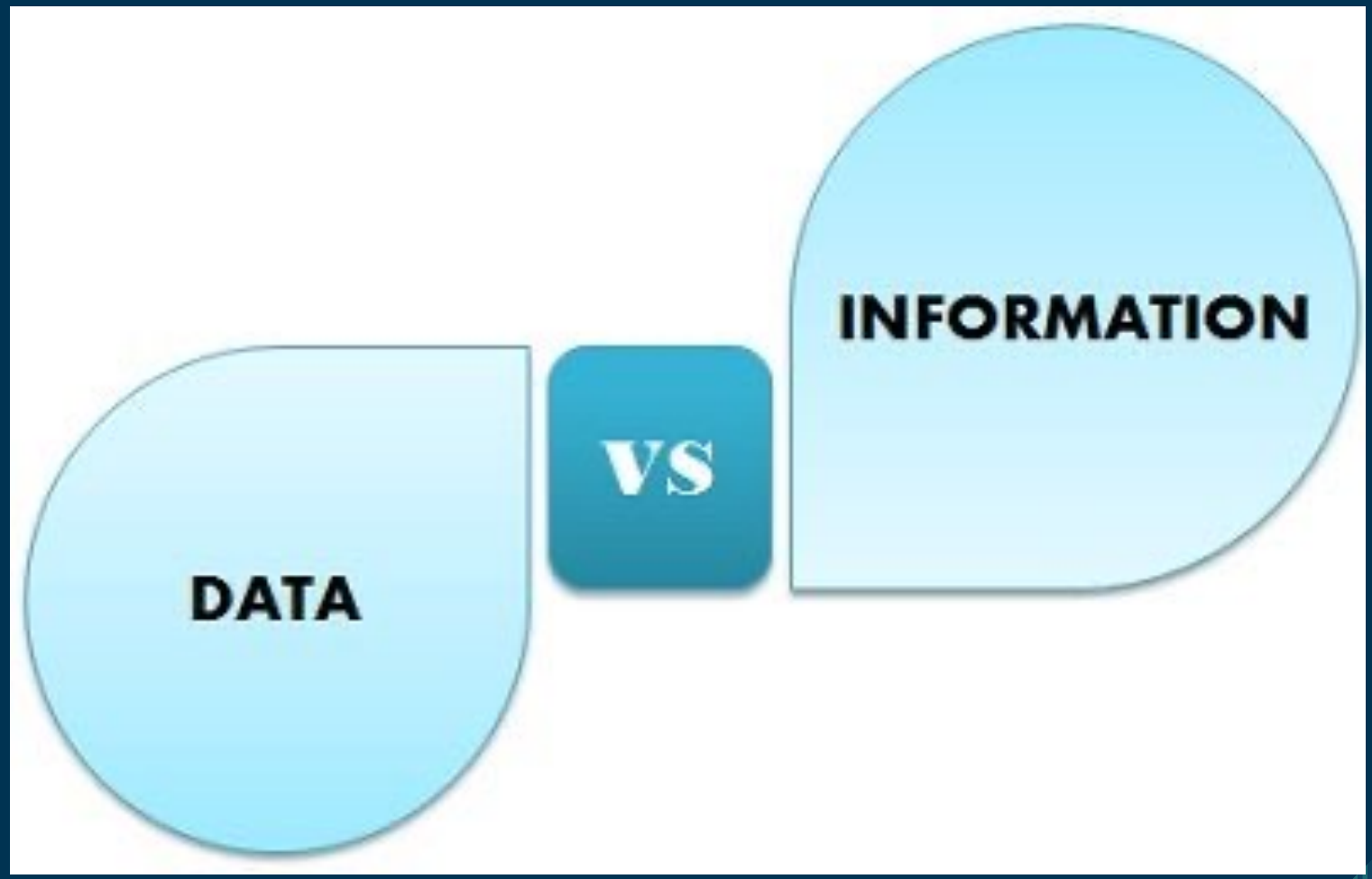
Một số thống kê

- Các ứng dụng có lỗ hỏng đã bị khai thác

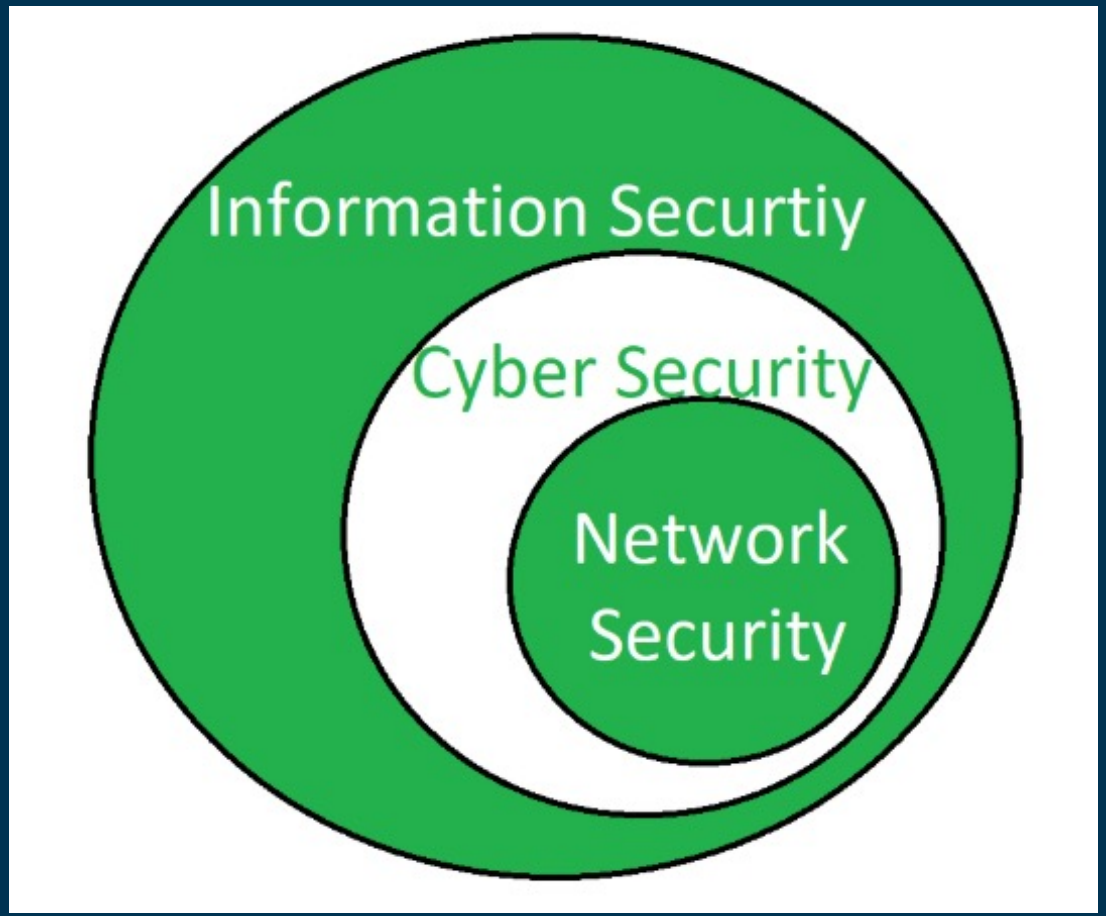


Source: Kaspersky Security Bulletin 2017

Một số Khái niệm



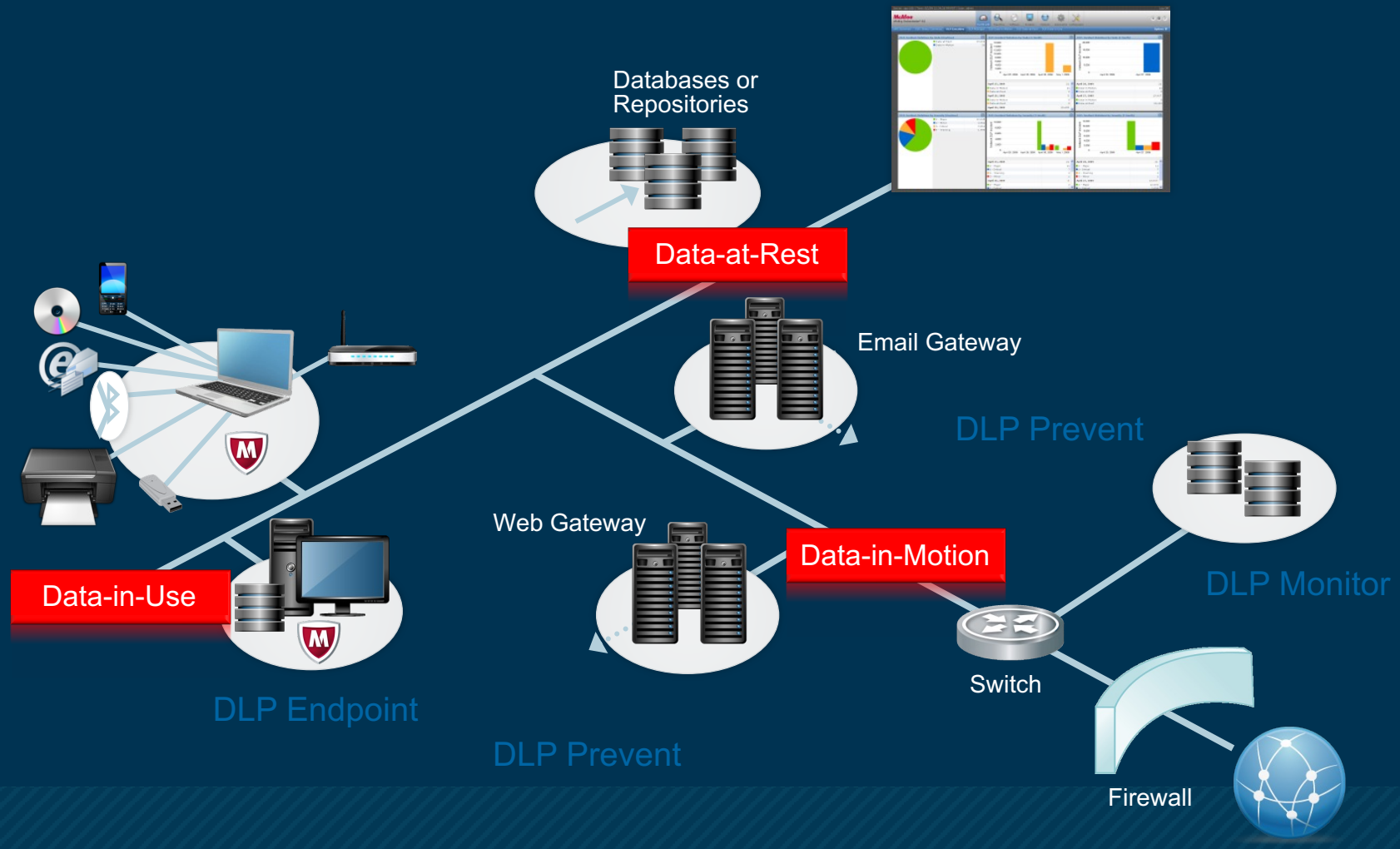
Một số Khái niệm



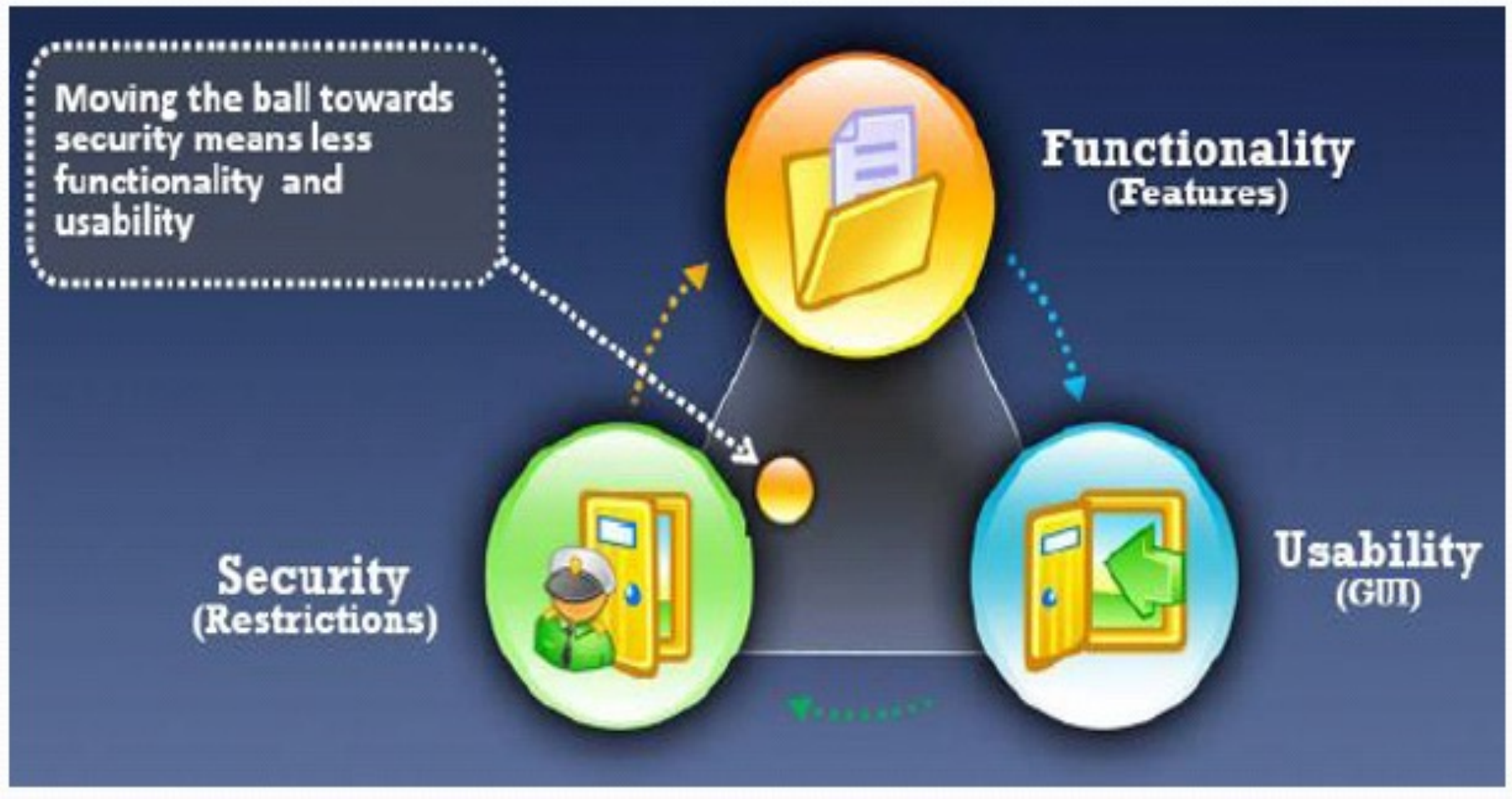
- Information Security vs. Cyber Security vs. Network Security?

Những đặc tính của thông tin

Trạng thái của thông tin



Mối quan hệ giữa Security, Functionality và Usability



Các tác nhân ảnh hưởng đến Thông tin?

Các tác nhân ảnh hưởng đến Thông tin?
Attacker

- Nghe lén trên mạng (Eavesdropping)
- Giả mạo IP Address (IP Address Spoofing)
- Tấn công Password (Password-Based Attacks)
- Tấn công từ chối dịch vụ (Denial-of-Service Attack)
- Tấn công tầng ứng dụng (Application Attack)
- Malicious Code
  - Virus
  - Worm
  - Trojan
  - Logic BOM
  - Rootkit
  - …

CÁC TÁC NHÂN ẢNH HƯỞNG ĐẾN THÔNG TIN?
NGƯỜI DÙNG

Hacker Vietnam có thể hack mà không cần tool

[redacted] Ông có biết là khi chat mà gõ password của mình thì nó sẽ hiện ra toàn dấu * ko?

[redacted] Thật hả?

[redacted] uh, ví dụ password của tui là ******, ông sẽ thấy nó chỉ là ****** thôi đúng ko?

[redacted]: hihi để tui thử xem. 123456

sao tui không thấy có dấu * nhỉ?

[redacted] đâu có, tui thấy ****** thôi

[redacted]: hihi hay thật, giờ tôi mới biết đó

[redacted] bất cứ khi nào ông gõ 123456 thì tôi chỉ thấy ****** mà thôi

[redacted]: khoan đã, sao ông biết password của tui là 123456

???

[redacted] À, ... tôi copy và paste cái đống ****** của ông vào, vì đó là password của ông nên ông sẽ thấy nó là 123456, còn tôi thì chỉ toàn thấy ****** thôi

[redacted] Tuyệt thật!, cám ơn ông nhiều nhé

CÁC TÁC NHÂN ẢNH HƯỞNG ĐẾN THÔNG TIN?
Tự NHIÊN

Phân loại dữ liệu

- Tại sao nên phân loại dữ liệu?
- Mục đích của phân loại dữ liệu?
- Những đối tượng nên phân loại dữ liệu?

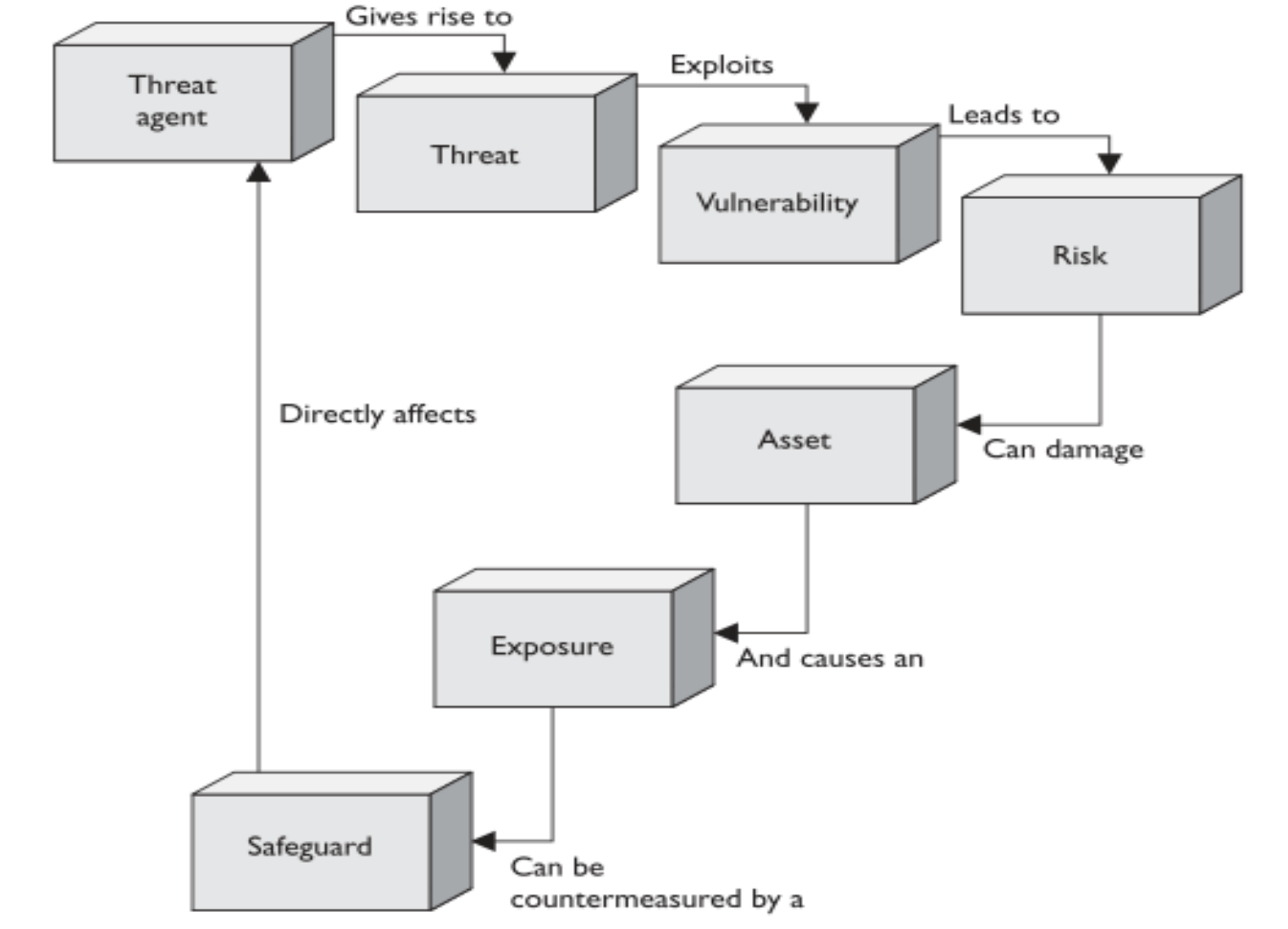
Phân loại dữ liệu (tt)

- Doanh nghiệp thương mại
  - Confidential
    - Bí mật thương mại, mã lập trình, thông tin mang tính cạnh tranh với các đối thủ,…
  - Private
    - Thông tin cá nhân
  - Sensitive
    - Thông tin tài chính, chi tiết dự án,….
  - Public
    - Mọi người đều có thể truy cập

Phân loại dữ liệu (tt)

- Quân đội
  - Top secret
    - Bản thiết kế vũ khí chiến tranh mới, thông tin gián điệp,…
  - Secret
    - Kế hoạch triển khai trong quản đội, vị trí bom hạt nhân,…
  - Confidential
    - Tình trạng sức khỏe lính sau trận đánh,…
  - Sensitive but unclassified
    - Thông tin y tế,…
  - Unclassified
    - Thông tin tuyển dụng,….

Mối quan hệ giữa các khái niệm trong an toàn, bảo mật



Mối quan hệ giữa các khái niệm trong an toàn, bảo mật

- Threat (mối đe dọa)
  - Hành động nguy hiểm khai thác những lỗ hổng
- Vulnerability (lỗ hổng)
  - Thiếu biện pháp đối phó hoặc trong biện pháp đối phó có điểm yếu
  - Phần cứng, phần mềm, qui trình và con người có thể bị khai thác
- Risk (rủi ro)
  - Threat Agent khai thác lỗ hổng và tác động tới hoạt động kinh doanh

Mối quan hệ giữa các khái niệm trong an toàn, bảo mật

- Exposure
  - Sự phơi bày dữ liệu dẫn đến sự chú ý của người tấn công.
- Control, countermeasure và Safeguard
  - Phương pháp làm giảm Risk

Các “nghề” trong an toàn thông tin

- Penetration Testing (Pentest)?
- IT Audit
- Bug Bounty?
- Hacker?
- Security Reseacher?
- …

Luật an toàn thông tin mạng VN

- Số: 86/2015/QH13
- 54 điều
  - Chú ý điều 7: “Các hành vi bị nghiêm cấm”
- 8 chương
- Áp dụng: 01/7/2016
- Luật này quy định về hoạt động an toàn thông tin mạng, quyền, trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng.

Luật an toàn thông tin mạng VN

Điều 7: Các hành vi bị nghiêm cấm:

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

Luật an toàn thông tin mạng VN

Điều 7: Các hành vi bị nghiêm cấm:

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

Luật an toàn thông tin mạng VN

Điều 7: Các hành vi bị nghiêm cấm:

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

Luật an ninh mạng - VN

- Số: 24/2018/QH14

(*Luật này được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV, kỳ họp thứ 5 thông qua ngày 12 tháng 6 năm 2018)*

- 7 chương
- 43 điều
  - Chú ý điều 8: Các hành vi bị nghiêm cấm về an ninh mạng
- Áp dụng: 01/01/2019
- Luật này quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan

Luật an ninh mạng - VN

Điều 8: các hành vi bị nghiêm cấm:

1. Sử dụng không gian mạng để thực hiện hành vi sau đây:

a) Hành vi quy định tại khoản 1 Điều 18 của Luật này;

b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

e) Xúi giục, lôi kéo, kích động người khác phạm tội.

Luật an ninh mạng - VN

Điều 8: các hành vi bị nghiêm cấm:

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

3. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

Luật an ninh mạng - VN

Điều 8: các hành vi bị nghiêm cấm:

4. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

5. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

6. Hành vi khác vi phạm quy định của Luật này.

Xử lý vi phạm

Điều 8/9: **Xử lý vi phạm pháp luật về an toàn thông tin mạng**

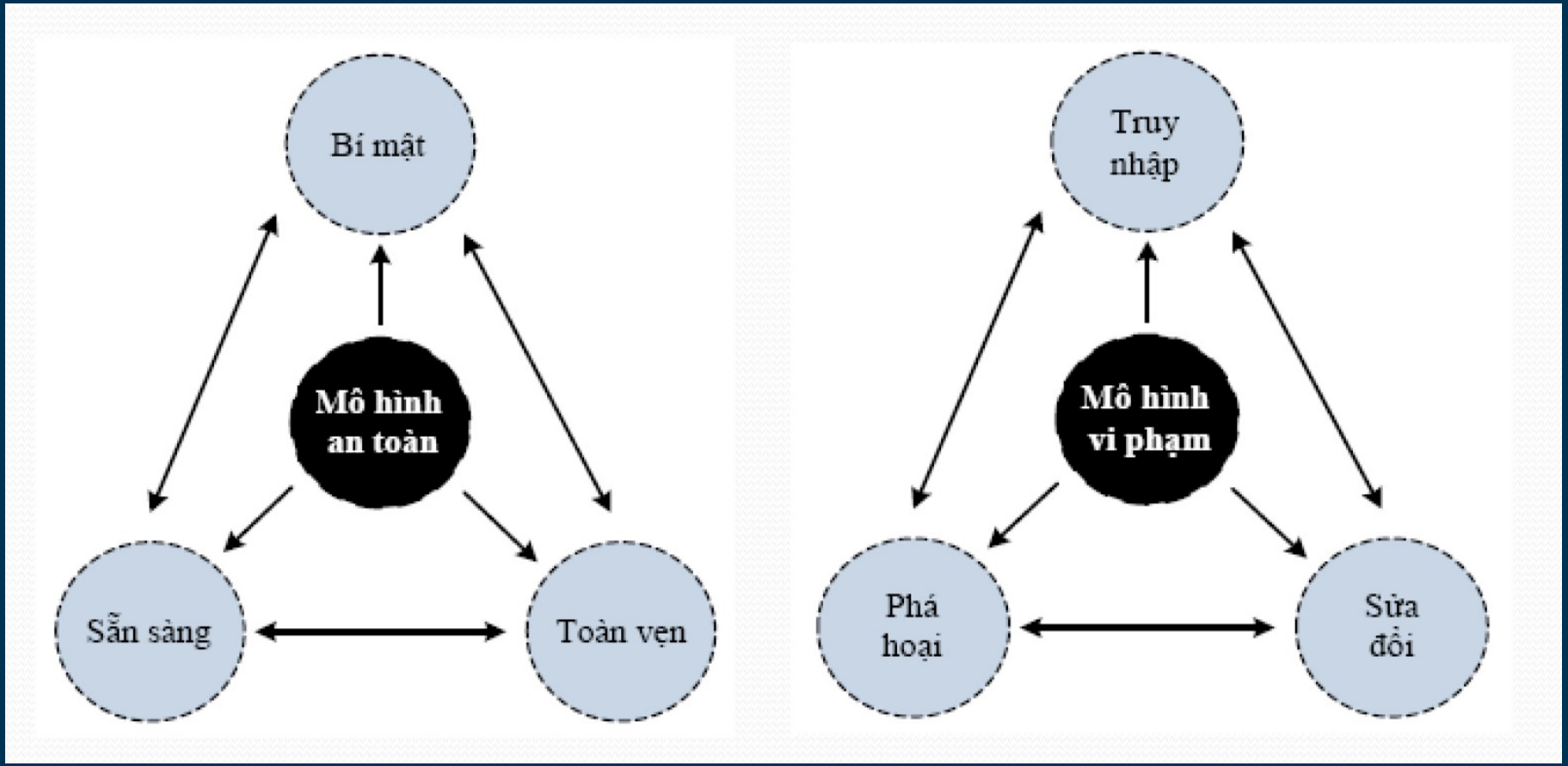
- Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

Nhận thức về Luật

- Nhận thức của sinh viên trong vấn đề tuân thủ pháp luật liên quan đến an toàn thông tin mạng?
  - Ranh giới giữa vi phạm và không vi phạm để có hành vi đúng
  - Luật ở mỗi Quốc gia/vùng lãnh thổ sẽ khác nhau
  - …

CIA

- **Confidentiality, Integrity, Availability**



CIA

- **Confidentiality**: Bí mật - **Integrity**: Toàn vẹn - **Availability**: Sẵn sàng
- Ba nguyên tắc cốt lõi này phải dẫn đường cho tất cả các hệ thống an ninh mạng.
- CIA cung cấp một bộ công cụ đo (tiêu chuẩn đánh giá) đối với các thực hiện an ninh.
- Mọi vi phạm bất kỳ một trong ba nguyên tắc này đều có thể gây hậu quả nghiêm trọng đối với tất cả các thành phần có liên quan.

CIA

- **Tính bí mật:**
  - Ngăn ngừa việc tiết lộ trái phép những thông tin quan trọng, nhạy cảm. Đó là khả năng đảm bảo mức độ bí mật cần thiết được tuân thủ và thông tin quan trọng, nhạy cảm đó dược phép che giấu với người dùng không được cấp phép.
  - Đối với an ninh mạng thì tính bí mật rõ ràng là điều đầu tiên được nói đến và nó thường xuyên bị tấn công nhất.
  - Các giải pháp:
    - Mã hóa dữ liệu ở trạng thái lưu trữ (Disk và Database)
    - Mã hóa dữ liệu trên đường truyền (IPSec, SSL, SSH, ...)
    - Quản lý truy cập (Vật lý và Logic)

CIA

- **Tính toàn vẹn:**
  - Toàn vẹn là sự phát hiện và ngăn ngừa việc sửa đổi trái phép dữ liệu, thông tin và hệ thống, do đó đảm bảo được sự chính xác của thông tin và hệ thống.
  - Các giải pháp:
    - Hashing (data security)
    - Quản lý cấu hình (system security)
    - Quản lý truy cập (Vật lý và Logic)

CIA

- **Tính sẵn sàng:**
  - Tính sẵn sàng bảo đảm các người sử dụng hợp pháp của hệ thống có khả năng truy cập đúng lúc và không bị ngắt quãng tới các thông tin trong hệ thống và tới mạng.
  - Tính sẵn sàng có liên quan đến độ tin cậy của hệ thống.
  - Các giải pháp:
    - RAID
    - Clustering
    - Load balancing
    - Redundant power
    - Backup
    - Disk shadowing
    - Roll-back functions
    - Fail-over configurations

AAA

- AAA: Access Control, Authentication, Auditing
- AAA, một khái niệm cơ bản về an ninh mạng, là một nhóm quy trình được sử dụng để bảo mật thông tin và là chiến lược nền tảng để thực thi các chính sách bảo mật trên mô hình CIA (một trong những mục tiêu của AAA là CIA)

AAA

Access Control:

- Có thể là một chính sách, phần mềm hay phần cứng làm nhiệm vụ cho phép hoặc từ chối đối tượng truy cập tài nguyên nào đó.
- Nó cũng có thể là một thiết bị tổng hợp: smart card, thiết bị sinh trắc học, router, …
- Hoặc cũng có thể là cách phân quyền trên các tập tin, thư mục chia sẻ trong hệ thống.

AAA

Authentication:

- Là quá trình thẩm định máy tính hoặc người dung đang có ý định truy cập vào hệ thống mạng hoặc tài nguyên mạng.
- Quá trình này đơn giản có thể là username/password hay phức tạp Kerberos, PAP, CHAP, …

AAA

Auditing:

- Là cơ chế theo dõi hoạt động của hệ thống ghi nhận các hành vi diễn ra trên hệ thống và liên kết các hành vi này với các tác nhân gây ra hành vi.

AAA

LƯU Ý:

- Cần phân biệt AAA trong ngữ cảnh quản lý mạng truy nhập máy chủ từ xa: Authentication, Authorization, Accounting để thực hiện quản lý truy nhập mạng của người sử dụng, theo dõi lưu lượng sử dụng và tính cước truy nhập. AAA trong trường hợp này thường triển khai cùng với các dịch vụ như RADIUS, TACACS+…

Khuôn mẫu an ninh
Security framework

- Security framework là một qui trình bảo mật được tạo bởi rất nhiều thực thể: cơ chế bảo vệ administrative, technical và physical, thủ tục, qui trình kinh doanh và con người cùng làm việc với nhau để cung cấp mức độ bảo mật cho môi trường hoạt động.

Khuôn mẫu an ninh
Security framework

- Một số framework phổ biến:
  - ISO/IEC 27000 Series
  - Enterprise Architecture Development
  - Security Controls Development (CobiT)
  - Process Management Development (ITIL)

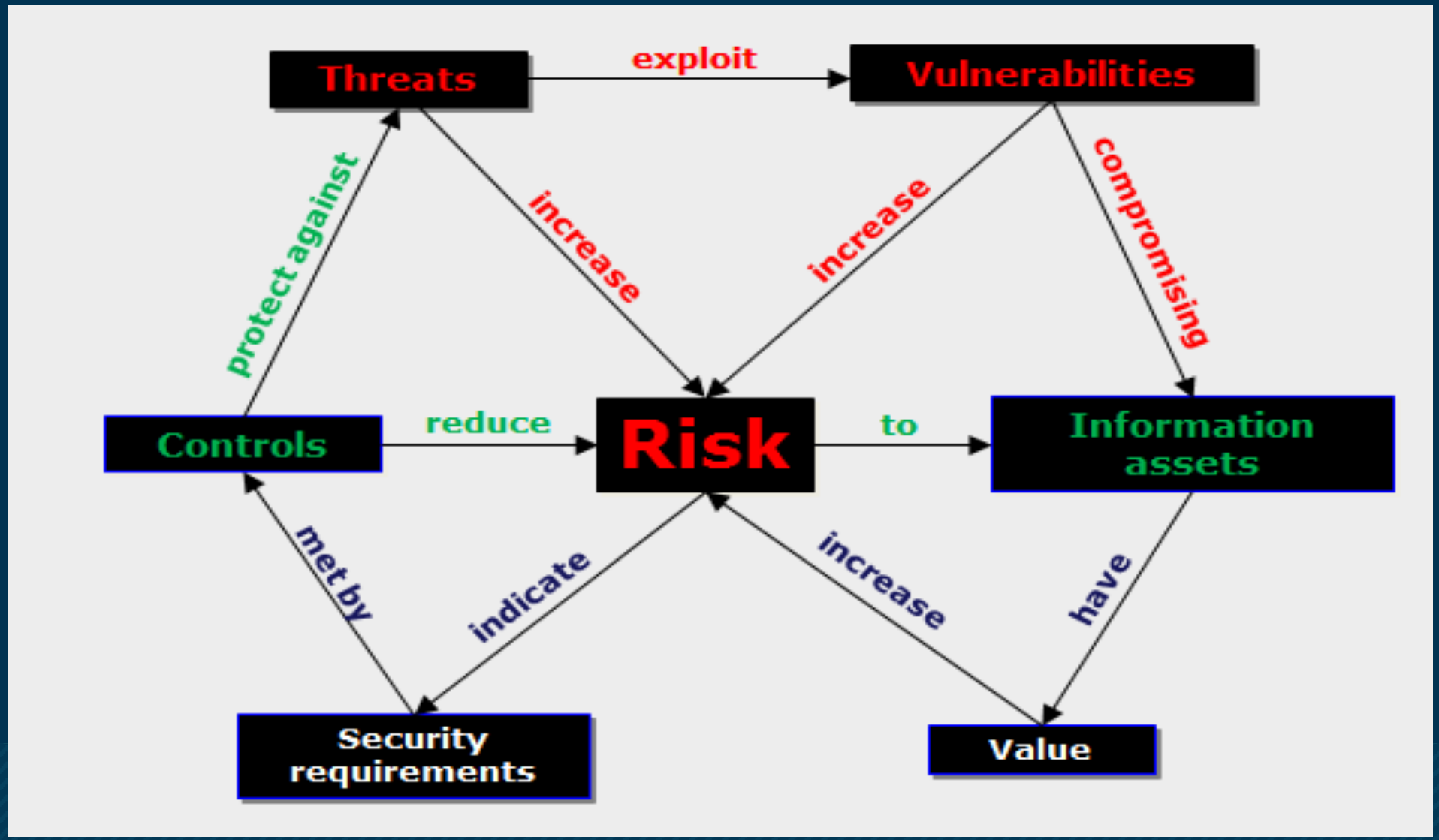
Quản lý rủi ro
Risk management

- Rủi ro trong bối cảnh an ninh là khả năng thiệt hại có thể xảy ra và hậu quả của thiệt hại đó khi xảy ra.
  - Physical damage
  - Human interaction
  - Equipment malfunction
  - Inside and outside attacks
  - Misuse of data
  - Loss of data
  - Application error

Quản lý rủi ro
Risk managment

- Quá trình phân tích rủi ro nhắm tới 4 mục tiêu:
  - Xác định tài sản và giá trị của tài sản
  - Xác định lỗ hổng bảo mật và mối đe dọa
  - Định lượng được khả năng và tác động của những đe dọa tới hoạt động kinh doanh
  - Cung cấp một sự cân bằng kinh tế giữa tác động của các mối đe dọa và chi phí các biện pháp đối phó.

Sơ đồ quan hệ rủi ro



Q&A

AN TOÀN MẠNG MÁY TÍNH

#01_TỔNG QUAN

ThS. Lê Đức Thịnh, UIT