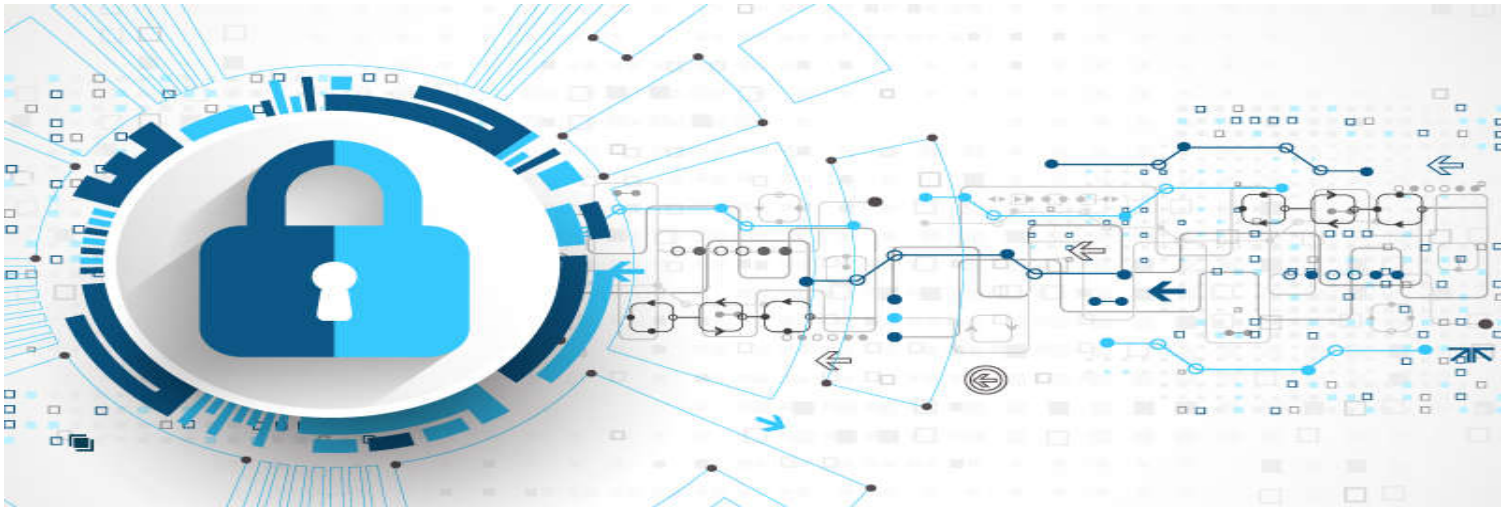
# Tập huấn bồi dưỡng kiến thức về An toàn, An ninh mạng năm 2021

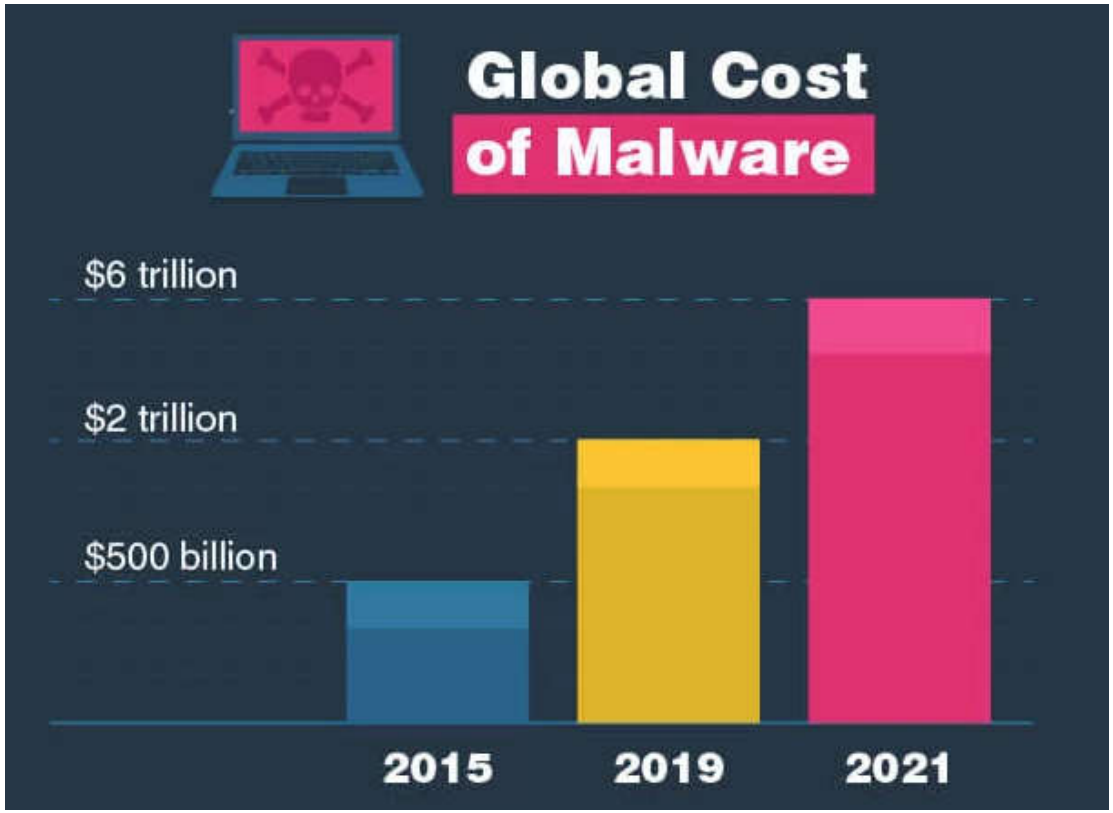


# HIỆN TRẠNG AN TOÀN THÔNG TIN

# TÌNH HÌNH ATTT THẾ GIỚI



Các con số



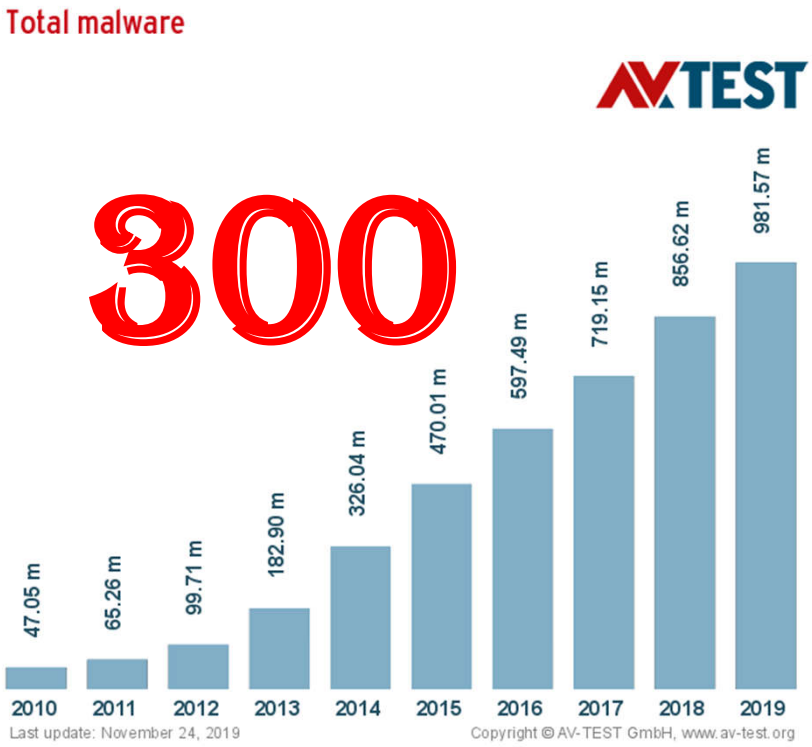

CYBERSECURITY VENTURES

1. United States (GDP: 20.49 trillion)
2. China (GDP: 13.4 trillion)
3. Japan: (GDP: 4.97 trillion)
4. Germany: (GDP: 4.00 trillion)
5. United Kingdom: (GDP: 2.83 trillion)
6. France: (GDP: 2.78 trillion)
7. India: (GDP: 2.72 trillion)
8. Italy: (GDP: 2.07 trillion)
9. Brazil: (GDP: 1.87 trillion)
10. Canada: (GDP: 1.71 trillion)

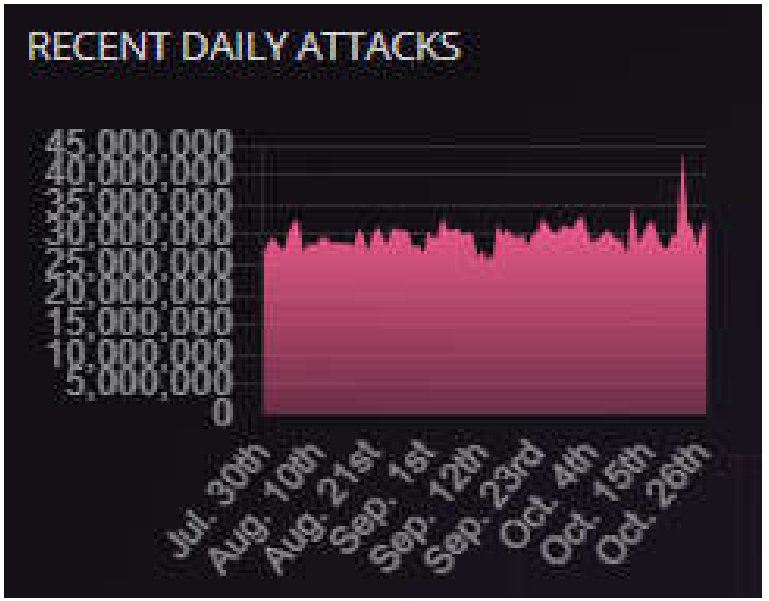
# TÌNH HÌNH ATTT THẾ GIỚI



Các con số: Lỗ hổng, mạng botnet




**500**





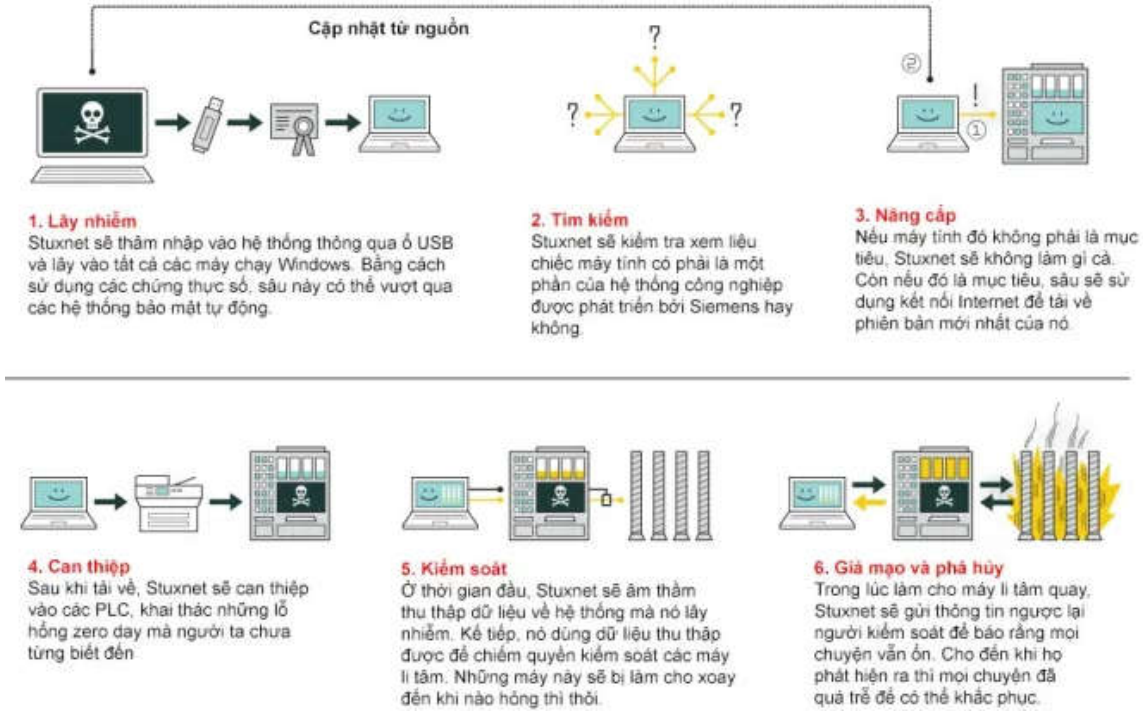

Trung bình có khoảng 500 cuộc tấn công mạng được ghi nhận trong mỗi giây và hơn 300 mã độc mới được tạo ra trong vòng một phút

# TÌNH HÌNH ATTT THẾ GIỚI



Các sự kiện nổi bật: Nhà máy lọc dầu ở Iran

## STUXNET - 2010




- ✓ Phát tán từ 6/2009 – phát hiện 12/7/2010
- ✓ 30.000 hệ thống máy tính đã bị nhiễm.
- ✓ 1/5máy ly tâm kiểu IR-1(tức khoảng 1.000 máy) Natanz
- ✓ Chương trình hạt nhân của Iran bị chậm lại 2 năm vì sâu Stuxnet.
- ✓ Chi phí tạo ra Stuxnet là 5-10 triệu USD và thiệt hại “nặng nề”

# TÌNH HÌNH ATTT THẾ GIỚI



Các sự kiện nổi bật: Mất điện ở Ucaina

**Black Energy - 12/2015**

**Tái diễn vào 12/2016**

**Ucraina**

¼ mạng lưới điện: 30 trạm biến áp (7 trạm 110kV, 23 trạm 25kV)

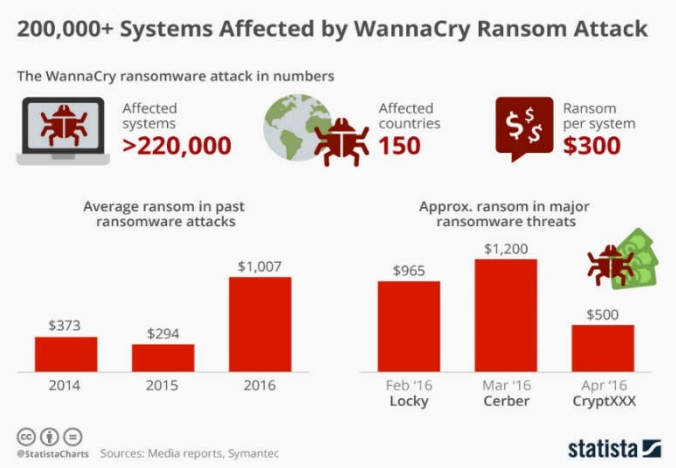
80.000 hộ ←→ 225.000 người

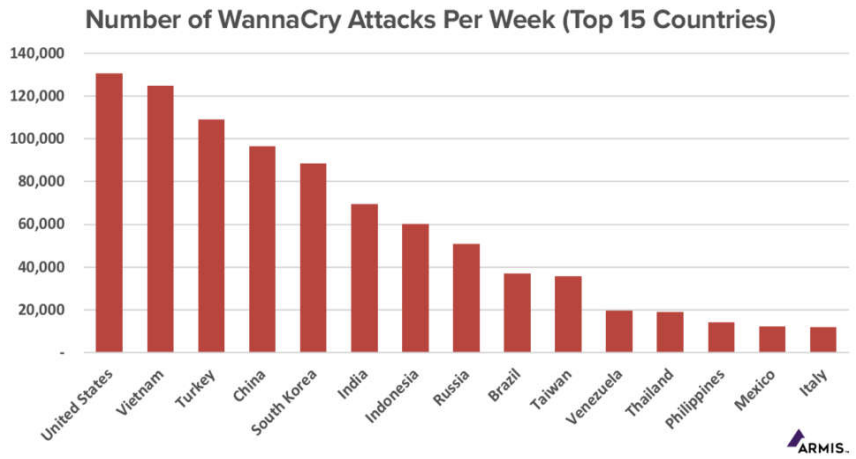
6 tiếng

# TÌNH HÌNH ATTT THẾ GIỚI



Các sự kiện nổi bật



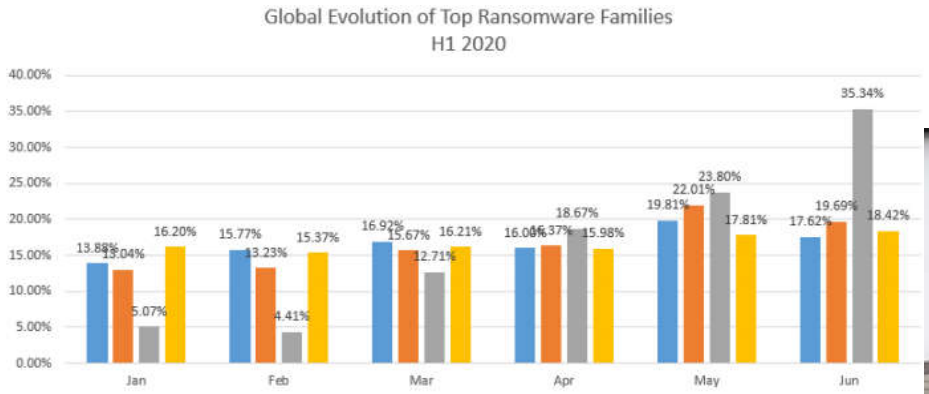



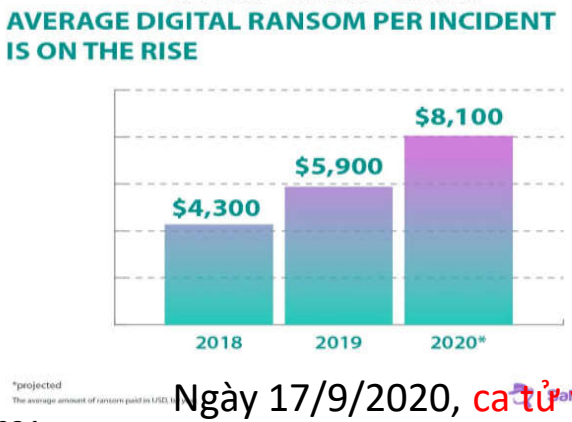

Cuộc tấn công ransomware WannaCry đã làm tê liệt hơn **300.000 máy tại 150 quốc gia, bao gồm 80 bệnh viện ở Anh**

# TÌNH HÌNH ATTT THẾ GIỚI



Các sự kiện nổi bật



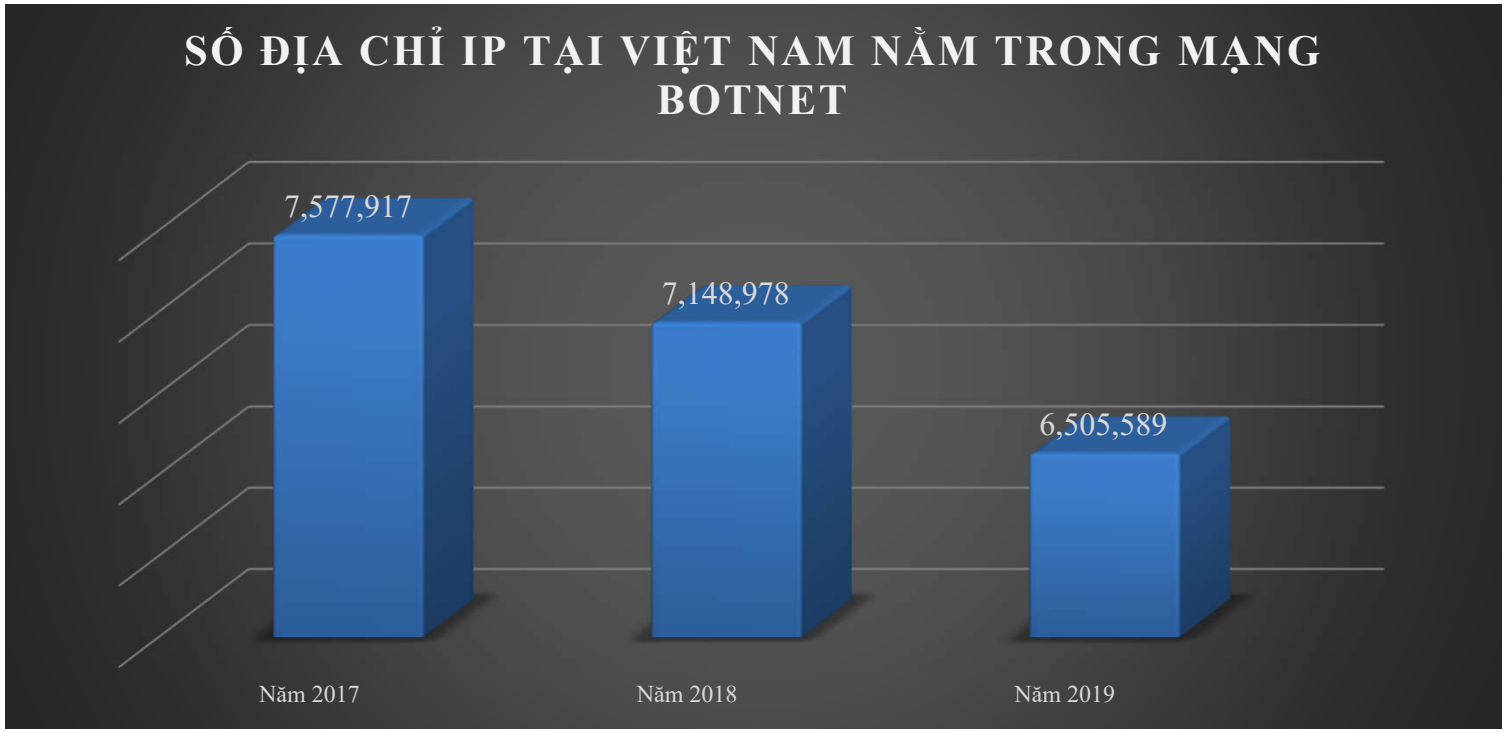


Ngày 17/9/2020, ca tử vong đầu tiên đã được ghi nhận sau một cuộc tấn công bằng mã độc tống tiền vào một bệnh viện ở Đức

# TÌNH HÌNH ATTT VIỆT NAM



Các con số



# TÌNH HÌNH ATTT VIỆT NAM



Sự kiện nổi bật: Tấn công mạng vào ngành Hàng không năm 2016 - 2017

Website bị chuyển hướng

Khoảng 100 chuyến bay bị hoãn

400.000 thông tin khách hàng bị rò rỉ

# TÌNH HÌNH ATTT VIỆT NAM



Sự kiện nổi bật

| Địa chỉ (Tên đơn vị) | Loại thẻ | Ngày giao dịch | Giờ giao dịch | Ngày xử lý |
|---|---|---|---|---|
| THEGIOIDIDONG.COM-1201 | GENT | 20160629 | 172623 | 20160701 |
| DIENMAYXANH.COM-663 | BNVN | 20160629 | 172635 | 20160701 |
| THEGIOIDIDONG.COM-1079 | GENT | 20160629 | 172640 | 20160701 |
| THE GIOI DI DONG-887 | MAST | 20160629 | 172642 | 20160701 |
| THEGIOIDIDONG.COM-1201 | GENT | 20160629 | 172807 | 20160701 |
| THEGIOIDIDONG.COM-1236 | BNVN | 20160629 | 172858 | 20160701 |
| THEGIOIDIDONG.COM-1201 | GENT | 20160629 | 172951 | 20160701 |
| THEGIOIDIDONG.COM-883 | BNVN | 20160629 | 173136 | 20160701 |
| THEGIOIDIDONG.COM-1201 | GENT | 20160629 | 173222 | 20160701 |
| THEGIOIDIDONG.COM-883 | BNVN | 20160629 | | |

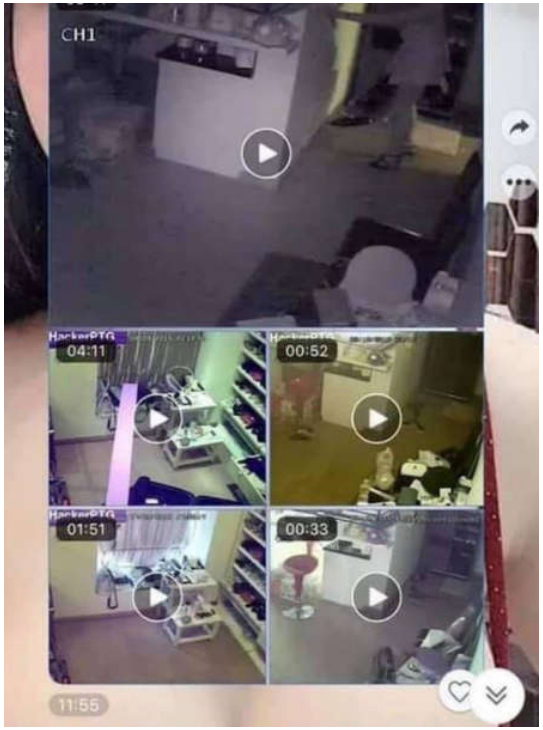
5,4 triệu khách hàng Thế Giới Di Động

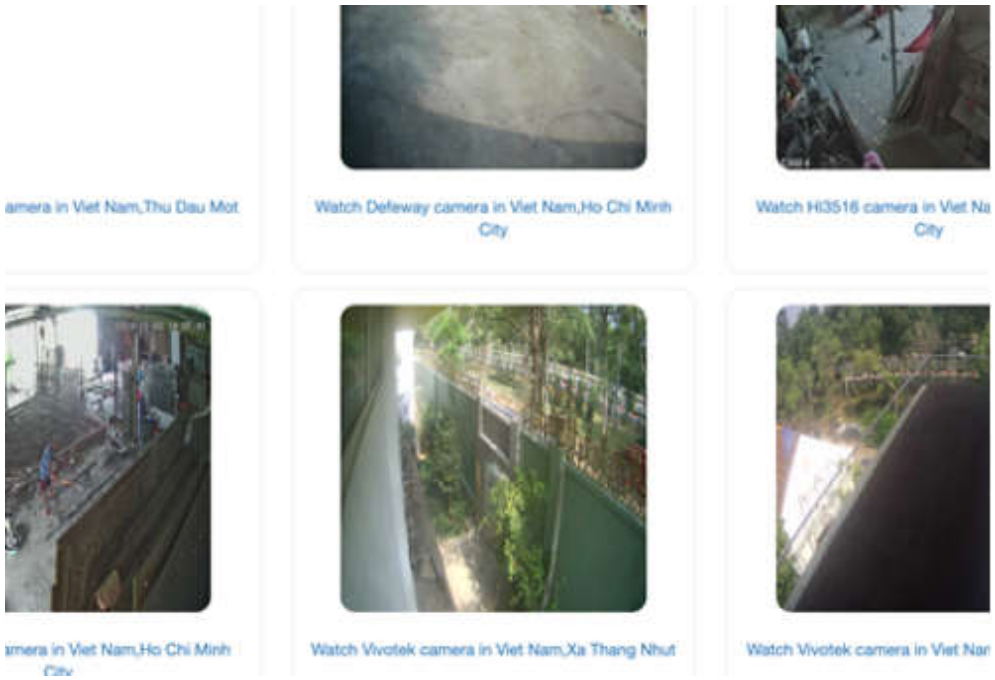

437.000 tài khoản Việt Nam bị lộ

# TÌNH HÌNH ATTT VIỆT NAM



Sự kiện nổi bật: Lộ camera an ninh



# TÌNH HÌNH ATTT VIỆT NAM



Thực tế

## The 10 Worst Botnet Countries

As of 29 June 2020 the world's worst botnet infected countries are:

| | | |
|---|---|---|
| 1 | India | Number of Bots: 2047650 |
| 2 | China | Number of Bots: 1419604 |
| 3 | Viet Nam | Number of Bots: 941401 |
| 4 | Iran (Islamic Republic of) | Number of Bots: 886746 |
| 5 | Brazil | Number of Bots: 586026 |

| | Country* | % of systems attacked |
|---|---|---|
| 1 | Vietnam | 69.6 |
| 2 | Algeria | 66.2 |
| 3 | Morocco | 60.4 |
| 4 | Indonesia | 60.1 |
| 5 | China | 59.5 |

Việt Nam trong top 20 nước bị mã độc tống tiền tấn công

**Việt Nam luôn trong "top" quốc gia dính mã độc nhiều nhất thế giới**

17:51 11/06/2018 - 0 - Hà Linh

CÔNG NGHỆ

**Việt Nam nằm trong top các nước bị tấn công mạng cao nhất thế giới**

**Việt Linh - Hà Bình (Ban Thời sự)** - Thứ hai, ngày 11/09/2017 15:11 GMT+7

# NGUYÊN NHÂN




01 Nhận thức về các nguy cơ mất an toàn thông tin đối với phần đông người Việt Nam còn chưa cao.

02 Tỷ lệ đầu tư cho ATTT so với phát triển ứng dụng CNTT còn thấp.

03 Phụ thuộc giải pháp công nghệ nước ngoài

# CÁC NGUY CƠ, RỦI RO

# Các nguy cơ, rủi ro



## Đe dọa trực tiếp tới mạng sống

## Hậu quả nhìn thấy được

# Nguy cơ trước các tổ chức tin tặc chuyên nghiệp



Báo cáo về các tổ chức APT


Virus
Adware
Keylogger
Ransomeware
WannaCry, Petya, ..
Worm
Botnet Control C&C
Control Panel
Fake
Zero Day Exploits
Trojans
Malware Industry
Ngành "Công nghiệp" mã độc
Underground Market

# Nguy cơ mã độc mã hóa đòi tiền chuộc (Ransomware)



Tấn công bằng mã độc Ransomware tăng cao

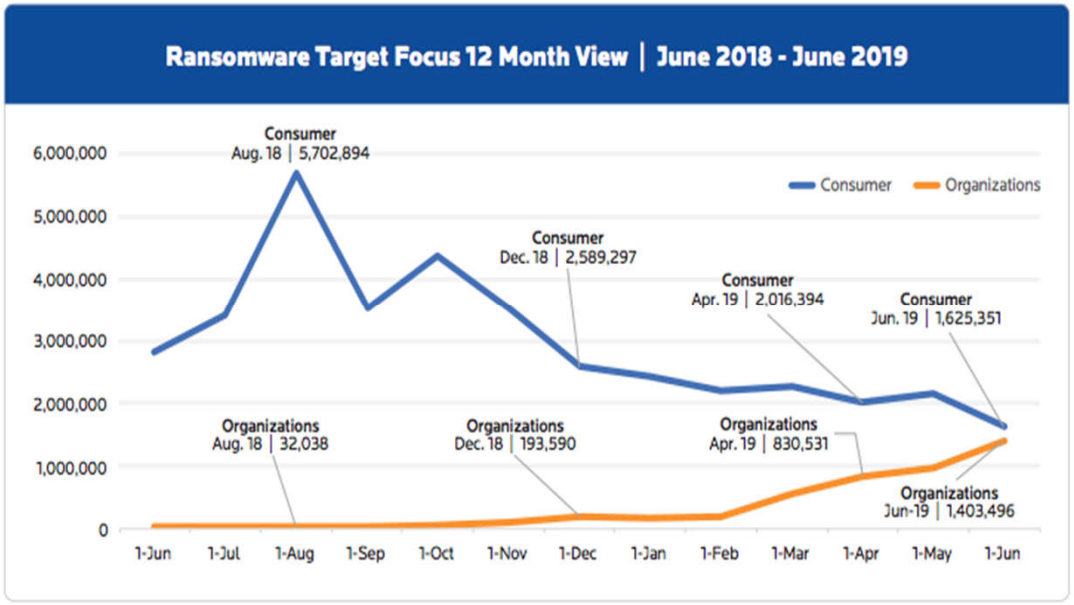



*Figure 2. Ransomware target shift from June 2018 to June 2019*

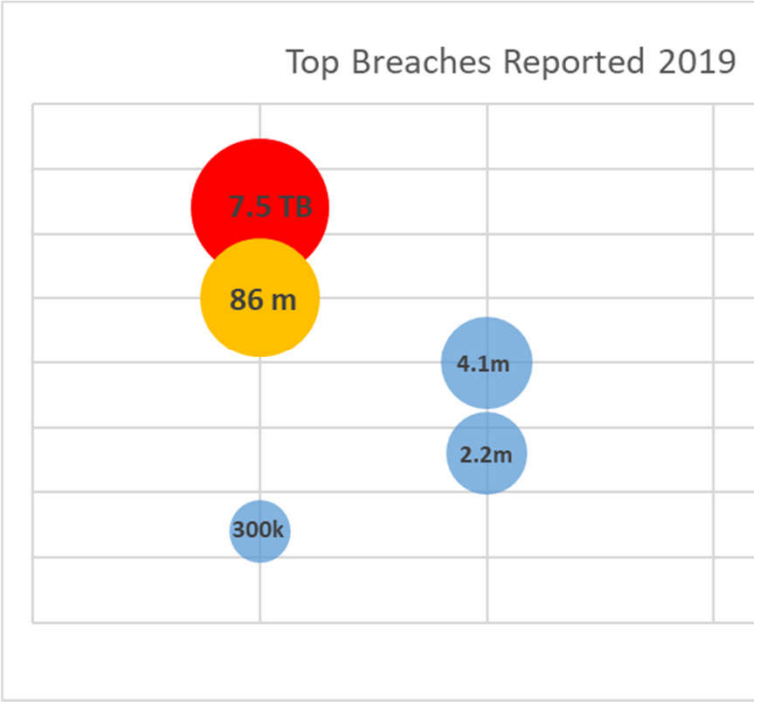
**9.6 days**

Average number of days a ransomware incident lasts

# Nguy cơ lộ lọt, vi phạm dữ liệu (Breaches)



Top các vụ vi phạm dữ liệu đầu năm 2019




Capital One breach is among the largest hacks of financial and insurance businesses

| YEAR | NAME | RECORDS BREACHED IN MILLIONS |
|---|---|---|
| 2017 | Equifax Corp. | 145.5 |
| 2009 | Heartland Payment Systems | 130 |
| **2019** | **Capital One Financial** | **106** |
| 2015 | Anthem | 80 |
| 2014 | J.P Morgan Chase | 76 |
| 2005 | CardSystems | 40 |
| 2015 | Experian | 15 |
| 2015 | Premera Blue Cross | 11 |
| 2015 | Excellus B.C.B.S. | 10 |
| 2007 | TD Ameritrade Holding Corp. | 6.3 |
| 2009 | CheckFree Corp. | 5 |
| 2015 | Scottrade | 4.6 |
| 2008 | Hannaford Bros. | 4.2 |
| 2018 | SunTrust Banks, Inc. | 1.5 |
| 2015 | CareFirst B.C.B.S. | 1.1 |
| 2008 | RBS WorldPay | 1.1 |

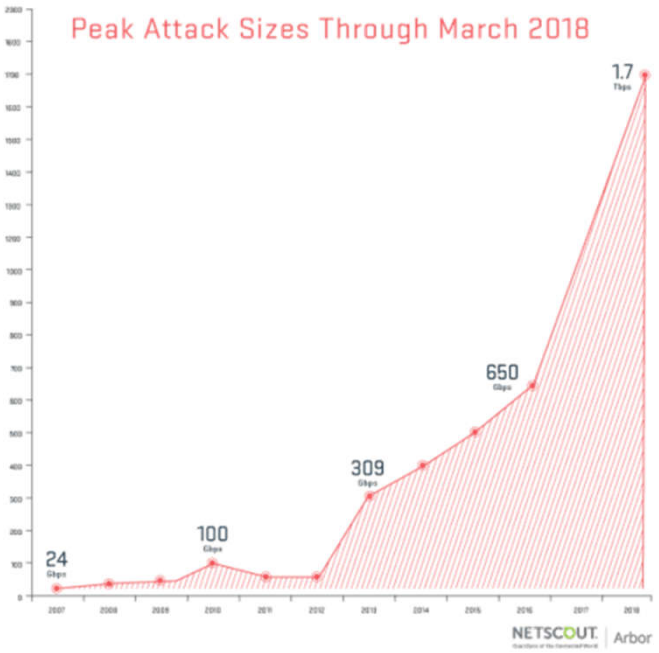
SOURCES: Privacy Rights Clearinghouse

AP

# Nguy cơ ảnh hưởng hoạt động của tổ chức



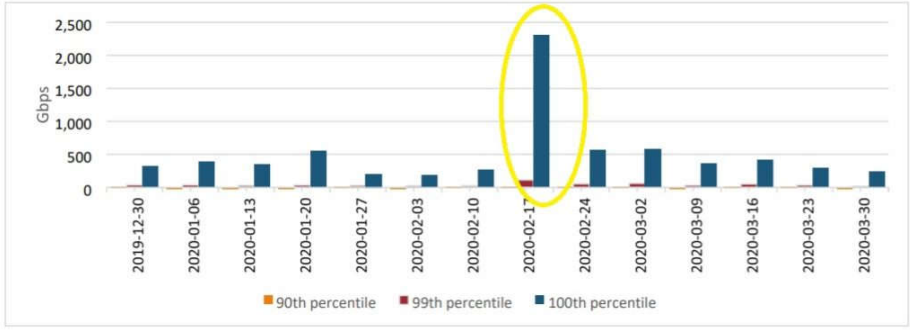
Ảnh hưởng đến các cơ quan tổ chức, các quốc gia





**2,3 Tbps**

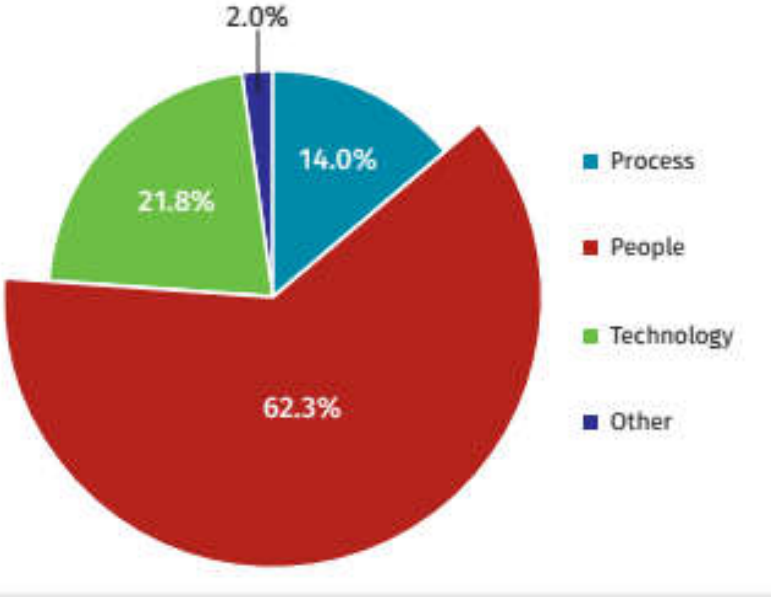
| Device | % of infected devices |
|---|---|
| MikroTik | 37.23% |
| TP-Link | 9.07% |
| SonicWall | 3.74% |
| AV tech | 3.17% |
| Vigor | 3.15% |
| Ubiquiti | 2.80% |
| D-Link | 2.49% |
| Cisco | 1.40% |
| AirTies | 1.25% |
| Cyberoam | 1.13% |
| HikVision | 1.11% |
| ZTE | 0.88% |
| Miele | 0.68% |
| Unknown DVR | 31.91% |

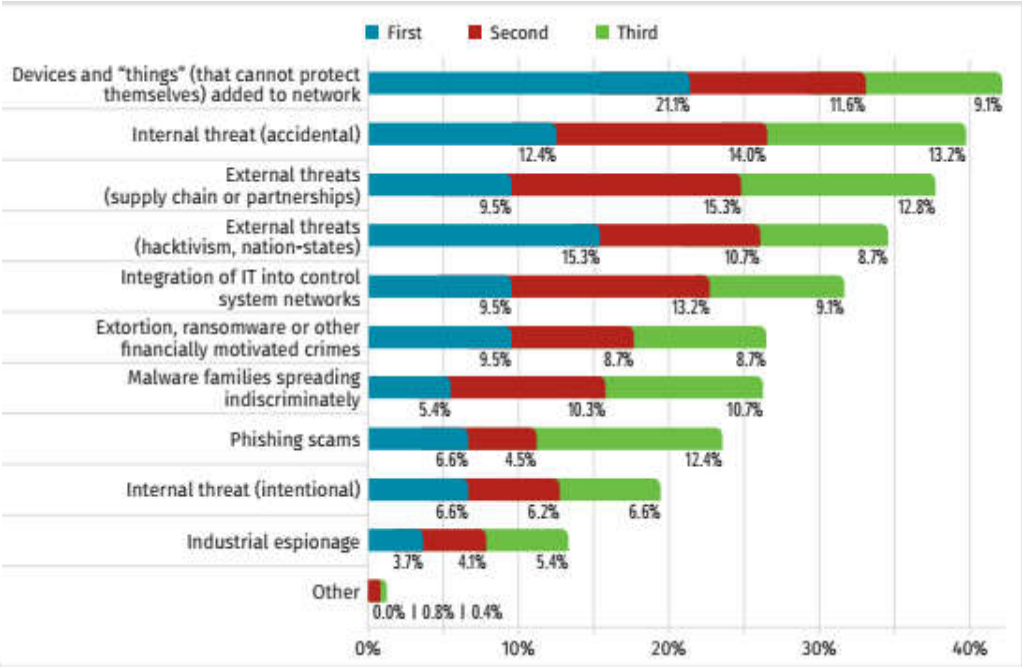


# Nguy cơ do con người



Lĩnh vực điện lực



# CÁC GIẢI PHÁP

# Công tác bảo đảm ATTT tại Việt Nam

**Hành lang pháp lý**

**Tổ chức, bộ máy**

**Biện pháp quản lý và kỹ thuật**

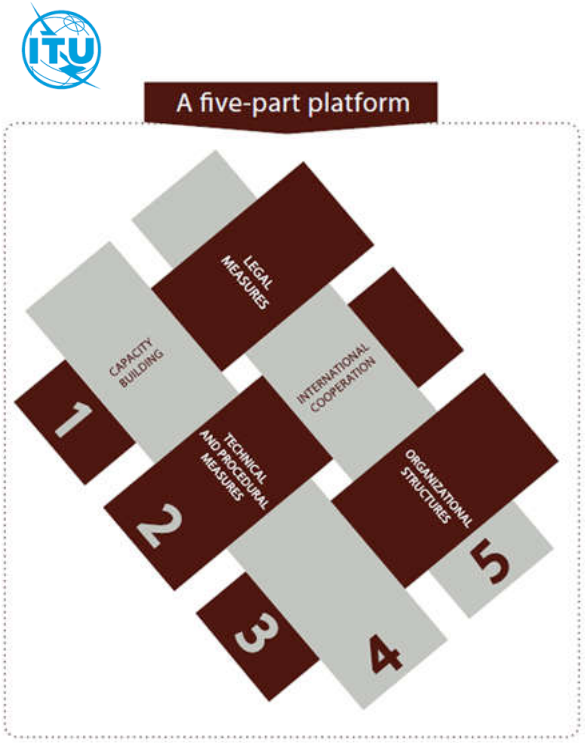
Quản lý: (1) Cấp phép; (2) Quy chế, chính sách; (2) Quy trình

Kỹ thuật: (1) Thiết bị bảo vệ; (2) Giám sát, phân tích, cảnh báo sớm; (3) Kiểm tra, đánh giá; (4) Kiểm định

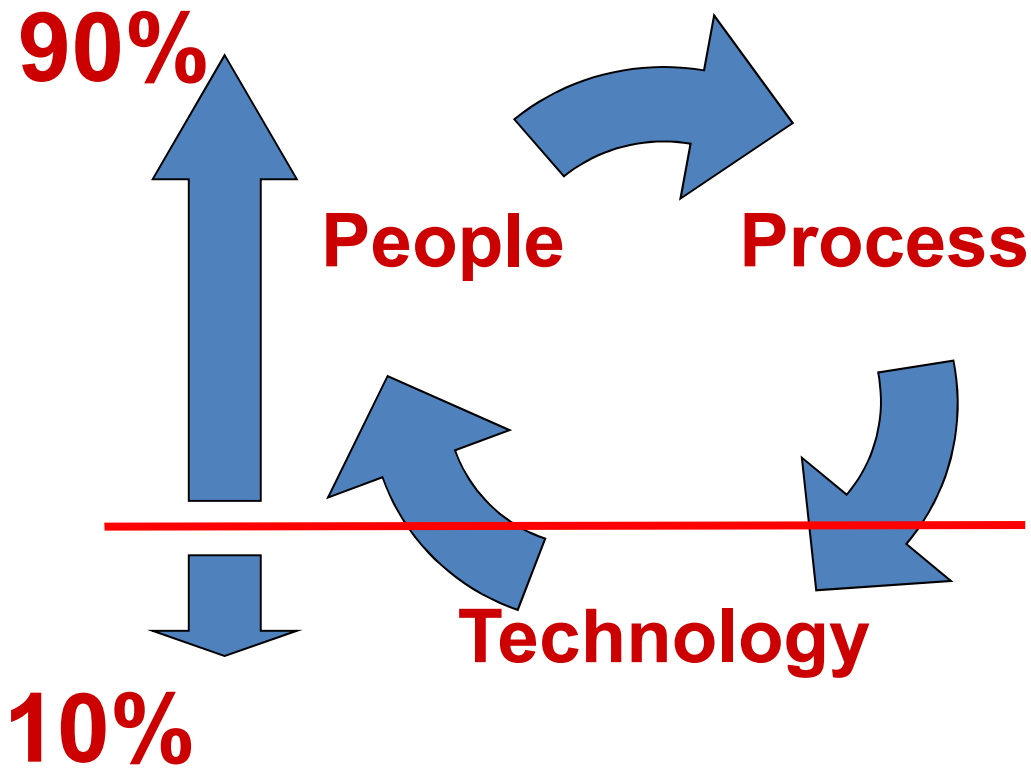
**Nâng cao năng lực**

Đào tạo, diễn tập, tuyên truyền, phổ biến

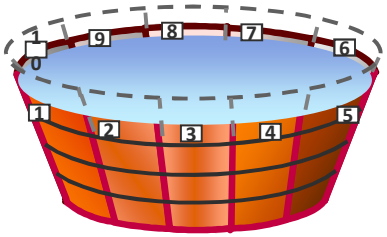
**Hợp tác trong nước và quốc tế**

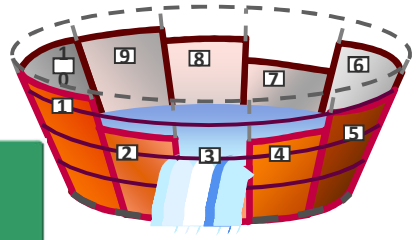


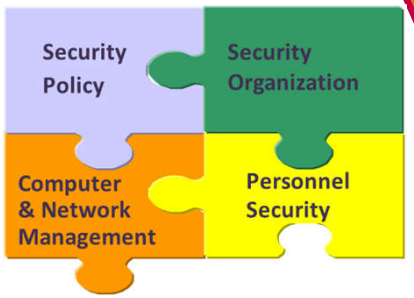
# Công nghệ và Con người




How much is Enough?



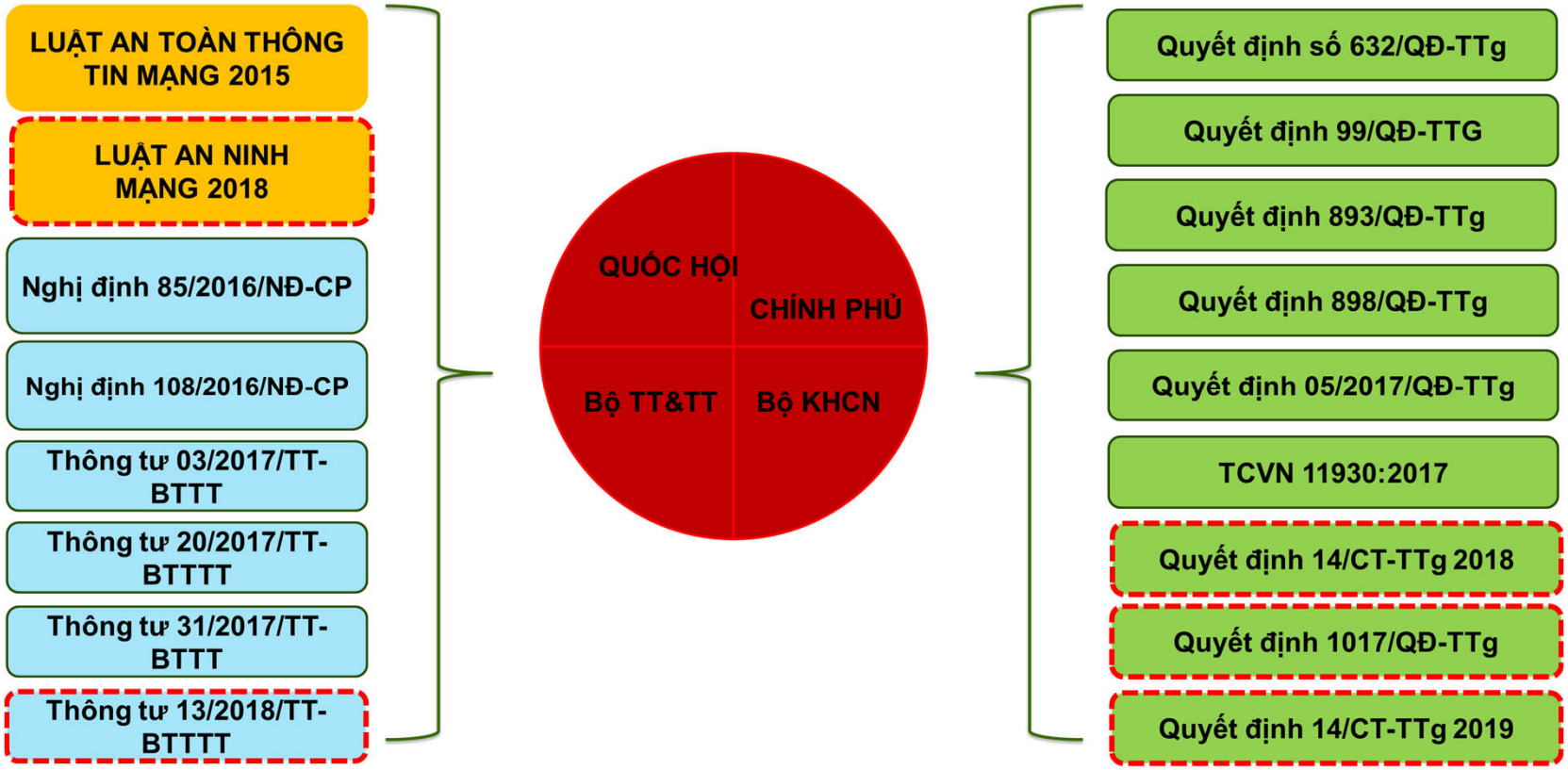




# HỆ THỐNG VĂN BẢN



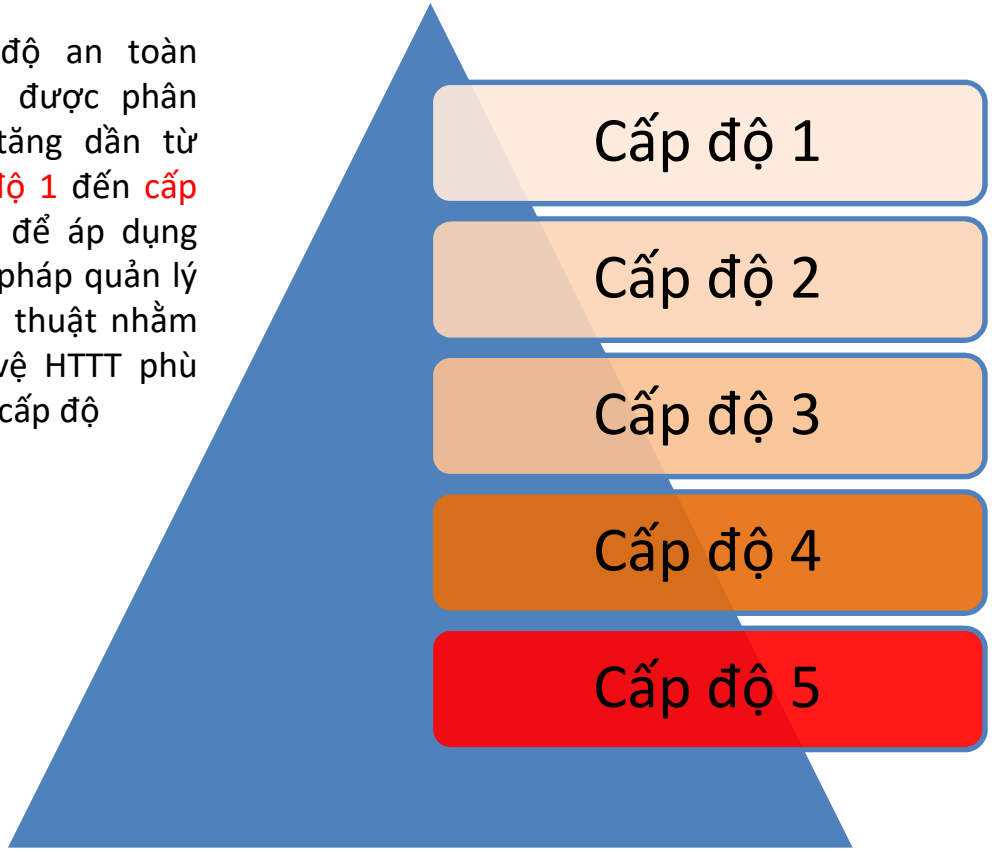
Văn bản quy phạm pháp luật về bảo đảm an toàn thông tin mạng



# Phân loại và xác định cấp độ



Cấp độ an toàn HTTT được phân loại tăng dần từ cấp độ 1 đến cấp độ 5 để áp dụng biện pháp quản lý và ký thuật nhằm bảo vệ HTTT phù theo cấp độ




- Cấp độ 1: Quyền và lợi ích hợp pháp của tổ chức, cá nhân
- Cấp độ 2: Quyền và lợi ích hợp pháp của tổ chức, cá nhân, lợi ích công cộng
- Cấp độ 3: Sản xuất, lợi ích công cộng, trật tự an toàn xã hội, quốc phòng, an ninh quốc gia
- Cấp độ 4: Lợi ích công cộng, trật tự an toàn xã hội, quốc phòng, an ninh quốc gia
- Cấp độ 5: Quốc phòng an ninh, quốc gia (tổn hại đặc biệt nghiêm trọng)

# Chỉ thị số 14/CT-TTg năm 2018



Thời hạn phải đáp ứng các yêu cầu các yêu cầu bảo đảm an toàn thông tin

**Chỉ thị 14/CT-TTg ban hành ngày 25/5/2018** chỉ thị các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương:

Khẩn trương phân loại, xác định cấp độ an toàn HTTT và xây dựng phương án bảo đảm an toàn HTTT theo cấp độ phù hợp với quy định của pháp luật và tiêu chuẩn, quy chuẩn kỹ thuật. Thời hạn hoàn thành HTTT cấp độ 4, 5 là **tháng 11/2018**

Bảo đảm có giải pháp phòng, chống mã độc bảo vệ cho 100% máy chủ, máy trạm, thiết bị đầu cuối liên quan và có cơ chế tự động cập nhật phiên bản hoặc dấu hiệu nhận dạng mã độc mới, hoàn thành **tháng 12/2018**

Định kỳ thực hiện kiểm tra, đánh giá tổng thể về an toàn thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 1/7/2016 của Chính phủ và hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông.

# Chỉ thị số 14/CT-TTg ngày 07/6/2019

**Bảo đảm tỷ lệ kinh phí 10% chi cho các SP, DV ATTT trong tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin hàng năm**

Tổ chức đánh giá và công bố định kỳ hàng năm mức độ an toàn thông tin mạng của Việt Nam

Bảo đảm an toàn, an ninh mạng theo mô hình 4 lớp thống nhất từ Trung ương đến địa phương

HTTT cấp độ 3 và cấp độ 4, định kỳ hàng năm thực hiện kiểm tra, đánh giá

Lực lượng tại chỗ; Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp; Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ; Kết nối, chia sẻ thông tin

# Nghị định 15/2020/NĐ-CP năm 2020



Xử lý các vi phạm hành chính trong môi trường bưu chính, viễn thông

**Lĩnh vực CNTT/ATTT (gồm 33 Điều, từ Điều 74 đến Điều 106), được chi ra thành các mảng Ứng dụng CNTT; An toàn thông tin mạng; Chống thư rác, tin nhắn rác và cung cấp dịch vụ nội dung**

**Hành vi vi phạm về ATTT mạng: Vi phạm các quy định về đảm bảo ATTT và ứng cứu sự cố ATTT mạng; bảo đảm ATTT cá nhân trên mạng; biện pháp giám sát an toàn, bảo vệ hệ thống thông tin; bảo đảm an toàn hệ thống thông tin theo cấp độ**

Góp phần ngăn ngừa hiệu quả thông tin sai sự thật: Điều 101, Nghị định 15 nêu rõ mức xử phạt vi phạm hành chính đối với hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin giả mạo, sai sự thật, …

Hạn chế tin nhắn rác, tăng chế tài xử phạt: Tại điểm b khoản 6 Điều 94 Nghị định 15/2020/NĐ-CP quy định: Tổ chức sẽ bị phạt tiền từ 60 - 80 triệu đồng khi có hành vi gửi hoặc phát tán tin nhắn rác, thư điện tử rác, phần mềm độc hại

# Hiện trạng bảo đảm an toàn, an ninh mạng hiện nay

## 1. Những kết quả đạt được

- **Hình ảnh quốc gia được cải thiện đáng kể**

**Năm 2021: Việt Nam đứng thứ 25 Thế giới, thứ 7 trong khu vực châu Á - Thái Bình Dương và thứ 4 khu vực ASEAN.**

- **Mạng lưới đơn vị chuyên trách, chuyên gia bước đầu đi vào hoạt động**

**200 cơ quan, tổ chức tại Việt Nam, trong đó có 22 bộ, cơ quan ngang bộ, 08 cơ quan thuộc Chính phủ, 63 Sở Thông tin và Truyền thông các tỉnh, thành phố, 17 tập đoàn, tổng công ty nhà nước, 45 ngân hàng và các tổ chức tài chính và 08 doanh nghiệp, tổ chức khác trong xã hội**

- **Hệ thống kỹ thuật quy mô quốc gia được triển khai**

**Hệ thống theo dõi, phát hiện xu hướng thông tin trên không gian mạng**

**Hệ thống điều phối, xử lý nguồn phát tán thông tin vi phạm pháp luật**

**Hệ thống theo dõi, thống kê tình hình lây nhiễm mã độc**

**Hệ thống chia sẻ và giám sát an toàn thông tin phục vụ chính phủ điện tử**

# Hiện trạng bảo đảm an toàn, an ninh mạng hiện nay

## 2. Tồn tại và hạn chế

- Mức độ quan tâm của người đứng đầu
- Kinh phí cho an toàn an ninh mạng
- Triển khai bảo đảm an toàn an ninh mạng chưa đúng cách

# Định hướng, cách thức triển khai mới

- An toàn, an ninh mạng ngay từ đầu, nâng cao sức "đề kháng"
  - An toàn, an ninh mạng ngay từ đầu, thường xuyên, liên tục
  - Nâng cao sức "đề kháng", thường xuyên, liên tục
- Triển khai bảo đảm an toàn, an ninh mạng nhiều lớp
  - "4 lớp" kỹ thuật: (1) Lớp mạng, (2) Lớp hệ điều hành và cơ sở dữ liệu, (3) Lớp ứng dụng và (4) Lớp thiết bị đầu cuối.
  - "4 lớp" tổ chức: (1) Lực lượng tại chỗ, (2) Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp, (3) Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ, (4) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.
- Triển khai hệ thống SOC hiệu quả
- Thúc đẩy hệ sinh thái Việt Nam, làm chủ công nghệ

# Thực thi bảo đảm an toàn thông tin cho hệ thống thông tin phục vụ phát triển CPĐT

**1. Xây dựng Hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo cấp độ**

**2. Triển khai Trung tâm điều hành an toàn, an ninh mạng**

**3. Kiểm tra, đánh giá an toàn thông tin**

**4. Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng**

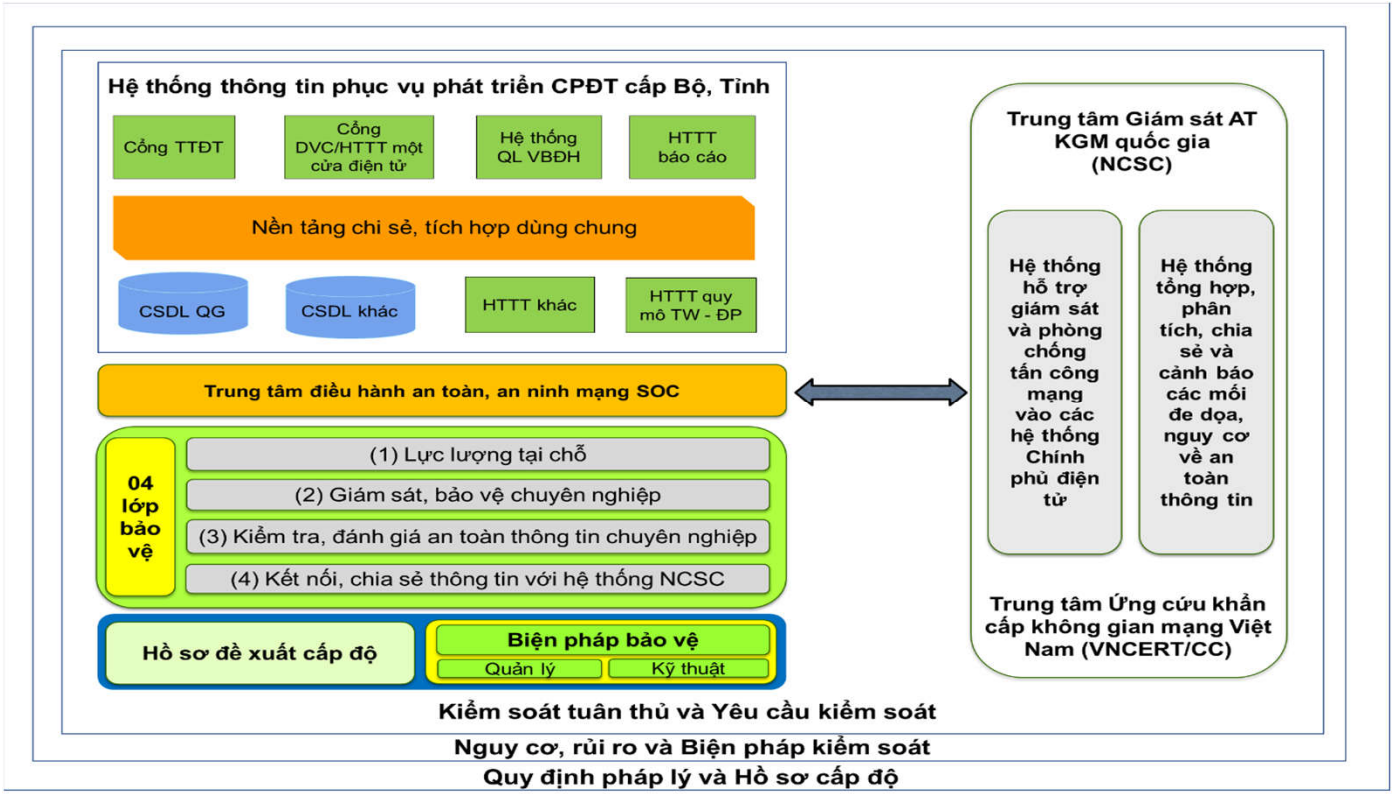
**5. Phòng, chống phần mềm độc hại**

# Xây dựng Hồ sơ đề xuất cấp độ và triển khai phương án bảo đảm an toàn thông tin theo cấp độ

**(1) Phương án bảo đảm an toàn thông tin trong HSĐXCĐ là sở cứ để đề nghị đầu tư nâng cấp hệ thống thông tin trong trường hợp hệ thống hiện tại chưa đáp ứng các yêu cầu an toàn theo quy định**

**(2) Phương án và kết quả thực hiện phương án bảo vệ trong HSĐXCĐ là cơ sở để cơ quan có thẩm quyền kiểm tra, đánh giá sự tuân thủ của cơ quan tổ chức đối với các quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ và đánh giá hiệu quả của phương án bảo vệ**

# Mô hình đảm an toàn thông tin tổng thể cấp bộ, tỉnh



# Mô hình đảm an toàn thông tin tổng thể cấp bộ, tỉnh

**Mô hình đảm an toàn thông tin tổng thể cấp bộ, tỉnh bao gồm các thành phần:**

**(1) Hệ thống thông tin phục vụ phát triển CPĐT, CQĐT và ĐTTM cấp bộ, tỉnh**

**(2) Trung tâm điều hành an toàn, an ninh mạng;**

**(3) Mô hình tổ chức "04 lớp" bảo đảm an toàn thông tin;**

**(4) Mô hình tham chiếu về biện pháp quản lý an toàn thông tin;**

**(5) Mô hình tham chiếu về giải pháp, công nghệ;**

**(6) Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng.**

# 4. Mô hình tham chiếu về biện pháp quản lý an toàn thông tin

# Mô hình tham chiếu phương án kỹ thuật bảo đảm an toàn thông tin

**a. Bảo đảm an toàn mạng**

**b. Bảo đảm an toàn máy chủ**

**c. Bảo đảm an toàn ứng dụng**

**d. Bảo đảm an toàn dữ liệu**

# Mô hình tham chiếu về giải pháp và công nghệ

## Các sản phẩm cụ thể được phân chia làm 08 nhóm, bao gồm:

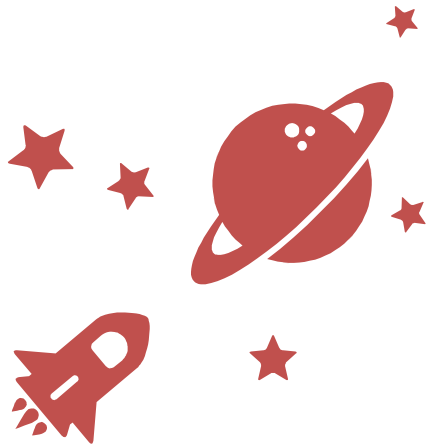
- Sản phẩm an toàn cho thiết bị đầu cuối
- Sản phẩm an toàn lớp mạng
- Sản phẩm an toàn lớp ứng dụng
- Sản phẩm bảo vệ dữ liệu
- Nhóm giải pháp định hướng phát triển theo hình thức cung cấp dịch vụ
- Sản phẩm trình duyệt
- Sản phẩm nền tảng tích hợp, chia sẻ dữ liệu
- Sản phẩm nền tảng điện toán đám mây

# Mô hình tham chiếu Trung tâm điều hành an toàn, an ninh mạng


**Công nghệ là các phương án, giải pháp kỹ thuật được sử dụng để bảo đảm việc giám sát an toàn thông tin đáp ứng các yêu cầu về kỹ thuật và tính hiệu quả.**

**Quy trình là những quy định trong quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức được xây dựng để phục vụ việc quản lý, vận hành hệ thống an toàn.**

**Con người là việc tổ chức nhân sự cán bộ chuyên trách, chuyên gia và các đội ngũ khác (nếu có) để vận hành quản lý hệ thống SOC và các thành phần liên quan.**



**Nâng cao mức độ bảo đảm an toàn, an ninh mạng của các cơ quan tổ chức gắn với việc thúc đẩy phát triển hệ sinh thái, làm chủ công nghệ bảo đảm an toàn, an ninh mạng của Việt Nam vì sự phát triển bền vững!**

# Trân trọng cảm ơn!