

# AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

**Nguyễn Tri Huy**

Phó Chủ tịch kiêm Tổng thư ký - Hội tin học tỉnh Khánh Hòa

# NỘI DUNG

- 01 THÁCH THỨC VỀ ATTT
- 02 THAY ĐỔI NHẬN THỨC VỀ ATTT
- 03 ƯU TIÊN HÀNG ĐẦU TRONG CHUYỂN ĐỔI SỐ
- 04 MỘT SỐ HƯỚNG TIẾP CẬN VÀ GIẢI PHÁP

**01**

**THÁCH THỨC  
VỀ AN TOÀN THÔNG TIN**

## THÁCH THỨC VỀ ANTT TRONG CHUYỂN ĐỔI SỐ



- Việc đảm bảo an toàn thông tin (ATTT) hay an ninh mạng (ANM) giờ đây đang là một nhiệm vụ quan trọng, yếu tố then chốt, ưu tiên, được thể hiện rõ trong các quan điểm, chiến lược và hành động cụ thể của tiến trình chuyển đổi số (CDS) quốc gia của Việt Nam.
  - Nền tảng số là không gian diễn ra các hoạt động của cơ quan, tổ chức, DN, người dân Việt Nam trên môi trường số. Vì vậy, công tác bảo đảm an toàn thông tin mạng cho các nền tảng số phải được coi là trọng tâm, ưu tiên hàng đầu; là nhiệm vụ gắn liền, không thể tách rời được trong quá trình chuyển đổi số.
- 
- Số liệu thống kê từ Bộ TT&TT cũng cho thấy, trong lĩnh vực an toàn thông tin, tỷ lệ doanh thu sản phẩm của DN Việt Nam so với sản phẩm nước ngoài tăng từ 18% (2015) lên 45% (2020) và năm 2021 đạt hơn 50%. Đáng chú ý, thị trường này đang được định giá doanh thu vào khoảng 2.300 tỷ đồng.
  - Theo Bộ TT&TT, hiện mức đầu tư cho an toàn thông tin ở Việt Nam đang còn thấp, chỉ chiếm khoảng 5% ngân sách đầu tư cho công nghệ thông tin, trong thời gian tới, Bộ sẽ thúc đẩy con số này lên khoảng 20%.
  - Một khảo sát của Hiệp hội An toàn thông tin cho thấy trong 2021 đã có đến 71% số lượng DN thành lập bộ phận an toàn thông tin, tăng mạnh so với 44% của năm 2020. Xấp xỉ 60% số DN có sử dụng các dịch vụ an toàn thông tin thuê ngoài và 50% trong số này đã chi 5% trong nguồn vốn công nghệ thông tin của mình cho hoạt động an toàn thông tin.
  - Theo thông tin từ Bộ Thông tin và Truyền thông, trên thế giới mới chỉ có khoảng 60% các dự án phát triển phần mềm áp dụng quy trình phát triển đánh giá ATTT trước khi vận hành. Tại Việt Nam, con số này còn thấp hơn rất nhiều. Vì vậy, vẫn còn tồn tại rất nhiều lỗi lập trình gây mất ATTT nghiêm trọng. Nếu những phần mềm này là các nền tảng số quốc gia thì hậu quả sẽ rất nghiêm trọng.

## THÁCH THỨC VỀ ANTT TRONG CHUYỂN ĐỔI SỐ



- Dữ liệu từ Bộ Công an cũng cho thấy, chỉ riêng 6 tháng đầu năm 2021, đã phát hiện 2.551 vụ tấn công mạng, 5,4 triệu lượt địa chỉ IP của các cơ quan Nhà nước bị tấn công bởi 15 biến thể mã độc. Cùng với đó là 1.555 vụ tấn công vào trang/cổng thông tin điện tử có tên miền .vn. Trong đó, 412 trang thuộc quản lý của cơ quan Nhà nước.
  - Hiện nay, ở nước ta thực tế cho thấy, đa số các thiết bị cá nhân như điện thoại thông minh, PC, laptop, máy tính bảng,... đều chứa rất nhiều rủi ro về an toàn thông tin mạng. Thậm chí các camera an ninh cũng chưa được đánh giá an toàn thông tin.
- 
- Có thể thấy các nguy cơ mất an toàn thông tin trước yêu cầu chuyển đổi số là thách thức không nhỏ đối với các cơ quan, tổ chức, doanh nghiệp. Không khó để bắt gặp thông tin về các cuộc tấn công mạng, đánh cắp dữ liệu được đăng tải trên các phương tiện truyền thông với mật độ phủ sóng dày đặc. Những lo ngại về việc bảo mật dữ liệu, bảo đảm an toàn thông tin trước yêu cầu chuyển đổi số không chỉ còn là nỗi lo của riêng các nhà chức trách, mà còn của doanh nghiệp, người dân.
  - Vì vậy, càng ý thức cao về sự không an toàn thì người dùng sẽ càng an toàn hơn. Nói cách khác, chỉ khi đảm bảo được an toàn, an ninh thông tin trên môi trường mạng thì công cuộc chuyển đổi số mới có thể được diễn ra toàn diện và bền vững.

**02**

**THAY ĐỔI NHẬN THỨC  
VỀ AN TOÀN THÔNG TIN**

## THAY ĐỔI NHẬN THỨC VỀ ATTT



An toàn thông tin liên quan đến các tính chất như sẵn sàng, bảo mật, toàn vẹn của thông tin. An toàn thông tin còn bao gồm các tính chất trách nhiệm, xác thực, tin cậy, xác nhận.

- ✓ Bảo mật là một trong những tính chất của hệ thống, nhằm xác định khả năng có thể tiếp cận và sử dụng thông tin của những đối tượng được xác thực.
- ✓ Tính chất đầy đủ và đúng đắn thuộc tính chất toàn vẹn của thông tin.
- ✓ Một trong những tính chất của an toàn thông tin chính là tính sẵn sàng. Tính sẵn sàng được hiểu có thể tiếp cận và sử dụng tùy theo nhu cầu của những đối tượng được phép.

- Một số vấn đề cần quan tâm khi triển khai hệ thống an toàn thông tin:

**Chính sách an ninh**

**Phòng/ban/nhóm/tổ chức an ninh**

**Phân loại và kiểm soát tài sản số**

**An ninh nhân sự**

**An ninh môi trường**

**Quản lý tác nghiệp và truyền thông**

**Kiểm soát truy cập**

**Duy trì và phát triển hệ thống**

**Quản lý sự liên tục**

**Quản lý rủi ro**

**Lập kế hoạch ứng phó sự cố**

**Duy trì tính tuân thủ**

## THAY ĐỔI NHẬN THỨC VỀ ATTT

- Nếu như trước đây, tất cả thông tin, dữ liệu của người dân được sao lưu và dự phòng trong văn bản giấy truyền thống thì khi CĐS toàn diện diễn ra, tất cả các tổ chức, cơ quan, với mọi thông tin của tổ chức, cá nhân đều được số hóa và lưu trữ trên những hệ phần mềm. Mọi hoạt động của tổ chức, cơ quan sẽ phụ thuộc hoàn toàn vào công nghệ từ Internet, hạ tầng mạng, phần mềm ứng dụng dịch vụ, những phát sinh lớn nhỏ... đều sẽ ảnh hưởng đến quá trình hoạt động bình thường của tổ chức đó.
- Nếu các đơn vị, tổ chức không có chiến lược, không có phương án bảo vệ dữ liệu cho phù hợp thì nguy cơ về mất ATTT sẽ khiến họ phải sẽ phải trả giá rất lớn. Do đó, tổ chức và người dân cần có sự chuẩn bị về nguồn lực, về kỹ thuật, về con người để bảo vệ thông tin, dữ liệu, đồng thời sẵn sàng ứng phó với các sự cố ATTT xảy ra. Đảm bảo được những điều này sẽ giúp cho các đơn vị, tổ chức cũng như dân có niềm tin để tham gia môi trường số, phục vụ phát triển kinh tế và xã hội.



**Trong giải pháp hay kế hoạch CĐS thì chúng ta cần xác định ATTT là then chốt để CĐS thành công và là vấn đề xuyên suốt, không thể tách rời trong CĐS.**



**03**

**ƯU TIÊN HÀNG ĐẦU  
TRONG CHUYỂN ĐỔI SỐ**

## ƯU TIÊN HÀNG ĐẦU TRONG CHUYỂN ĐỔI SỐ

- Việt Nam đã và đang bước vào cuộc cách mạng số và CDS đã trở thành động lực chính để phát triển kinh tế xã hội, do đó việc tham gia, làm chủ, chủ động xử lý các sự cố, vấn đề ANM không phải của riêng DN, giờ đây là trách nhiệm chung của toàn xã hội. Thực hiện tốt điều này, chúng ta góp phần đảm bảo thành công cho công cuộc CDS quốc gia và phấn đấu đưa Việt Nam trở thành trung tâm ANM khu vực ASEAN theo sự chỉ đạo của Thủ tướng Chính phủ về việc thực thi Chiến lược CDS toàn diện, trên mọi mặt đời sống xã hội.
- Một trong những điều kiện cần thiết giúp quá trình CDS diễn ra nhanh chóng là tạo được niềm tin và giải quyết được thách thức trong việc bảo vệ dữ liệu nhạy cảm của người dân và doanh nghiệp
- Tuy nhiên có 3 thực tế còn tồn tại hiện hữu
  - Tỷ lệ các hệ thống thông tin triển khai phương án bảo đảm an toàn thông tin theo cấp độ còn khiêm tốn.
  - Lừa đảo và tội phạm mạng ngày càng gia tăng.
  - Thiết bị số phục vụ chuyển đổi số ở các cấp đang sử dụng chưa được kiểm tra; hệ thống thông tin chưa được đánh giá an toàn.

**An toàn thông tin sẽ luôn là một yếu tố cần đánh giá trong quá trình lên ý tưởng, thiết kế và thực hiện các sáng kiến số để đảm bảo quá trình Chuyển đổi số thành công và an toàn.**



**04**

**MỘT SỐ HƯỚNG TIẾP CẬN VÀ GIẢI PHÁP  
CHO AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ**

## MỘT SỐ HƯỚNG TIẾP CẬN VÀ GIẢI PHÁP



### Một số hướng tiếp cận

1. Chuyển đổi số đi cùng bài toán chuyển đổi bảo mật, an toàn tài liệu lưu trữ điện tử.
2. Sử dụng dịch vụ ATTT thay vì đầu tư quá nhiều vào ATTT tự chủ ở giai đoạn đầu.
3. Tập trung vào quy trình và con người ATTT hơn là công cụ, công nghệ.
4. Phổ cập ATTT đến tất cả các cấp, các đối tượng thông qua các hình thức tuyên truyền, các nội dung đào tạo, tập huấn.

### Áp dụng mô hình PDCA trong triển khai hệ thống ATTT

- ✓ **Plan:** được hiểu là thiết lập các mục tiêu, chính sách an ninh, các quá trình và thủ tục hợp lý với việc quản lý rủi ro và cải tiến an ninh thông tin để phân phối các kết quả theo các chính sách và mục tiêu tổng thể của tổ chức.
- ✓ **Do:** điều hành và thi hành các dấu hiệu kiểm soát, chính sách an ninh, các quá trình và thủ tục.
- ✓ **Check:** kiểm soát và xem xét giúp đánh giá, đo lường hiệu năng của quá trình so với chính sách an ninh, tìm kiếm sự phù hợp, và báo cáo kết quả cho ban quản lý / lãnh đạo xem xét, áp dụng các thay đổi phù hợp.
- ✓ **Act:** duy trì và cải tiến, đưa ra các hành động khắc phục phòng ngừa dựa trên các kết quả xem xét giúp phát triển và cải tiến liên tục hệ thống.

## MỘT SỐ HƯỚNG TIẾP CẬN VÀ GIẢI PHÁP

### Một số giải pháp

1. Ngay từ khâu thiết kế, xây dựng kế hoạch CDS cần phải hoàn thiện ngay khâu ATTT, dành tối thiểu 10% ngân sách đầu tư CNTT hàng năm cho lĩnh vực này.
2. Phải nâng cao nhận thức về ATTT. Đây là một yếu tố mà các tổ chức phải nhận thức rõ, ATTT là sự phát triển lợi ích quốc gia trên không gian số.
3. Các tổ chức, DN cũng cần phải đảm bảo ATTT theo mô hình 4 lớp, từ trung ương tới địa phương, tổ chức, giám sát bảo vệ chuyên nghiệp, kiểm tra định kỳ kết nối, chia sẻ với các hệ thống quốc gia, giám sát định kỳ hệ thống chuyên nghiệp từ đó thúc đẩy sự tham gia thị trường ATTT tại Việt Nam.
4. Việc phát triển, ứng dụng các sản phẩm / giải pháp phục vụ ATTT phải do Việt Nam làm chủ công nghệ, ưu tiên các giải pháp "Made in Vietnam".
5. Phải thoát cách làm "hồng đầu vá đẫy" - Đây là cách làm bị động, luôn đi sau các đối tượng tấn công.
6. Việc bảo đảm an toàn thông tin cho các nền tảng số phải được thực hiện ngay từ khâu thiết kế, như là một trong những tính năng quan trọng nhất của sản phẩm. An toàn thông tin được chú trọng suốt quá trình phát triển và vận hành nền tảng, tuân thủ theo quy trình phát triển - vận hành an toàn. Kiên quyết áp dụng nguyên tắc, hệ thống chưa kết luận bảo đảm an toàn thông tin thì chưa đưa vào sử dụng.



***TRÂN TRỌNG CẢM ƠN!***

**AN TOÀN ĐỂ CHUYỂN ĐỔI  
CHUYỂN ĐỔI PHẢI AN TOÀN**

Thông tin liên hệ:

**Nguyễn Tri Huy – Phó Chủ tịch kiêm Tổng thư ký**

**Hội tin học tỉnh Khánh Hòa**

**Điện thoại / Zalo: +84.903500600**

**Email: [huy@kaict.org.vn](mailto:huy@kaict.org.vn)**