Tạp chí điện tử
Khoa học và Công nghệ Giao thông
Trang website: https://jstt.vn/index.php/vn

Data security challenges in online education: requirements for information technology human resources in the context of digital transformation

Nguyen Duc Toan[1], Ngo Thi Oanh[2*], Trinh Thị Thu Hang[3]
[1]Vietnam Women's Academy, Hanoi, Vietnam
[2]Vietnam Women's Academy, Hanoi, Vietnam
[3]Faculty of Law and Politics, University of Transport Technology, Hanoi, Vietnam

Article info
Type of article:
Original research paper

DOI:
https://doi.org/10.58845/jstt.utt.2026.vn.6.2.116-125

***Corresponding author:**
Email address:
oanh.ngo@hvpnvn.edu.vn

Received: 12/01/2026
Received in Revised Form: 24/02/2026
Accepted: 05/03/2026

Abstract: This study examines data security challenges in online education in Vietnam in the context of rapid digital transformation. The expansion of online learning platforms has exposed educational institutions to increasingly complex cybersecurity threats, including ransomware attacks, phishing campaigns, large-scale personal data breaches, and distributed denial-of-service (DDoS) attacks. These risks not only violate data protection regulations but also significantly undermine institutional reputation, learner trust, and the goal of developing a secure and sustainable digital education system. The research adopts the NIST Cybersecurity Framework (NIST CSF 2.0) as its core theoretical foundation to comprehensively assess the current situation, identify key vulnerabilities, and propose a multi-stakeholder coordination model. In this model, information technology (IT) personnel play a central role in facilitating collaboration among university leadership, administrative units, faculty members, and students. Quantitative analysis is conducted using mathematical models such as aggregated risk assessment formulas, Poisson distribution for estimating incident probability, and logistic models for evaluating response effectiveness and improvements in security culture. The findings indicate that human factors constitute the most critical vulnerability, particularly limited awareness, reluctance to report incidents, and insufficient coordination skills. Moreover, regular cybersecurity exercises (4–6 times per year) are identified as the most practical and effective solution to shift from a “static” security posture to a “dynamic” and proactive one. Based on these findings, the study proposes a new competency framework for IT human resources, emphasizing the integration of technical expertise, governance capacity, and soft skills, thereby contributing to the development of a secure and sustainable digital education ecosystem in Vietnam.

Keywords: Data security; online education; NIST framework; IT human resources; cybersecurity exercises; digital transformation; quantitative risk analysis; multi-stakeholder coordination model.

Tạp chí điện tử
Khoa học và Công nghệ Giao thông
Trang website: https://jstt.vn/index.php/vn

Thách thức bảo mật dữ liệu trong đào tạo trực tuyến: Yêu cầu đối với nguồn nhân lực Công nghệ thông tin trong bối cảnh chuyển đổi số

Nguyễn Đức Toàn[1], Ngô Thị Oanh[2*], Trịnh Thị Thu Hằng[3]
[1]Học viện Phụ nữ Việt Nam, Hà Nội, Việt Nam
[2]Học viện Phụ nữ Việt Nam, Hà Nội, Việt Nam
[3]Trường Đại học Công nghệ Giao thông vận tải, Hà Nội, Việt Nam

Thông tin bài viết
Dạng bài viết:
Bài báo nghiên cứu

DOI:
https://doi.org/10.58845/jstt.utt.2026.vn.6.2.116-125

***Tác giả liên hệ:**
Địa chỉ Email:
oanh.ngo@hvpnvn.edu.vn

Ngày nộp bài: 12/01/2026
Ngày nộp bài sửa: 24/02/2026
Ngày chấp nhận: 05/03/2026

Tóm tắt: Nghiên cứu này phân tích các thách thức bảo mật dữ liệu trong đào tạo trực tuyến tại Việt Nam trong bối cảnh chuyển đổi số giáo dục diễn ra mạnh mẽ. Sự phát triển nhanh chóng của các nền tảng học trực tuyến đã kéo theo nhiều rủi ro an ninh mạng ngày càng phức tạp, bao gồm tấn công mã độc tống tiền, lừa đảo qua email, rò rỉ dữ liệu cá nhân quy mô lớn và tấn công từ chối dịch vụ. Những rủi ro này không chỉ vi phạm các quy định pháp lý về bảo vệ dữ liệu cá nhân mà còn ảnh hưởng nghiêm trọng đến uy tín của cơ sở giáo dục, niềm tin của người học và mục tiêu xây dựng hệ thống giáo dục số an toàn, bền vững. Nghiên cứu sử dụng Khung an ninh mạng NIST CSF 2.0 làm nền tảng lý thuyết để đánh giá toàn diện thực trạng, xác định các lỗ hổng và đề xuất mô hình phối hợp đa bên, trong đó nhân sự công nghệ thông tin đóng vai trò trung tâm trong việc điều phối giữa các chủ thể như lãnh đạo nhà trường, các phòng ban chức năng, giảng viên và sinh viên. Phương pháp phân tích định lượng được triển khai thông qua các mô hình toán học như công thức rủi ro tổng hợp, phân phối Poisson và mô hình logistic nhằm đo lường xác suất xảy ra sự cố, thời gian ứng phó và hiệu quả cải thiện văn hóa bảo mật. Kết quả nghiên cứu chỉ ra rằng yếu tố con người là điểm yếu lớn nhất, thể hiện ở nhận thức hạn chế, tâm lý ngại báo cáo và thiếu kỹ năng phối hợp. Đồng thời, việc tổ chức diễn tập an ninh mạng định kỳ (4–6 lần mỗi năm) được xác định là giải pháp hiệu quả nhất nhằm chuyển từ trạng thái bảo mật "tĩnh" sang "động", nâng cao khả năng phản ứng và giảm thiểu rủi ro. Trên cơ sở đó, nghiên cứu đề xuất khung năng lực mới cho nhân lực công nghệ thông tin, góp phần xây dựng hệ sinh thái giáo dục số an toàn và bền vững tại Việt Nam.
Từ khóa: Bảo mật dữ liệu, đào tạo trực tuyến, khung NIST, nhân lực CNTT, diễn tập an ninh mạng, chuyển đổi số, phân tích rủi ro định lượng, mô hình phối hợp đa bên.

1. Giới thiệu

Chuyển đổi số trong lĩnh vực giáo dục tại Việt Nam đã trở thành một quá trình tất yếu, mang tính chiến lược và diễn ra với tốc độ chưa từng có, đặc biệt sau đại dịch COVID-19. Từ một quốc gia với tỷ lệ sử dụng Internet chỉ khoảng 40% vào năm 2019, đến năm 2025, tỷ lệ này đã tăng vọt lên hơn 78,8% dân số, tương đương hơn 80 triệu người dùng

Internet thường xuyên [1] [2]. Sự bùng nổ này đã mở ra cơ hội lớn cho giáo dục trực tuyến: hơn 85% các cơ sở giáo dục đại học đã triển khai ít nhất một nền tảng học tập trực tuyến như Moodle, Google Classroom, Microsoft Teams, Canvas, hoặc các hệ thống quản lý học tập tùy chỉnh nội địa. Các nền tảng này không chỉ hỗ trợ học tập từ xa mà còn tích hợp quản lý điểm số, bài tập, tài liệu giảng dạy, thi cử trực tuyến, và thậm chí quản lý hành chính học đường. Các văn bản chỉ đạo quan trọng của Đảng và Nhà nước, bao gồm Nghị quyết 52-NQ/TW năm 2024 về định hướng phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia, cùng Nghị quyết 29-NQ/TW năm 2025 [3] về đổi mới căn bản, toàn diện giáo dục và đào tạo, đã xác định rõ giáo dục số là một trong những trụ cột chiến lược để xây dựng nguồn nhân lực chất lượng cao cho nền kinh tế tri thức, hướng tới mục tiêu đưa Việt Nam trở thành quốc gia số vào năm 2030 và có tầm nhìn phát triển đến năm 2045 [4].

Tuy nhiên, sự phát triển nhanh chóng và quy mô lớn của giáo dục số đã kéo theo những thách thức bảo mật dữ liệu nghiêm trọng và ngày càng phức tạp. Theo các báo cáo an ninh mạng uy tín năm 2025, Việt Nam đang đối mặt với làn sóng tấn công mạng tinh vi, đa dạng và có tổ chức. Tổng số cuộc tấn công mạng ghi nhận trong năm 2025 ước tính khoảng 552.000 vụ, dù giảm 19% về số lượng so với năm trước nhưng mức độ thiệt hại kinh tế và xã hội tăng mạnh đáng kể, với 52,3% tổ chức bị ảnh hưởng nghiêm trọng [5]. Ngành giáo dục đặc biệt dễ bị tổn thương và liên tục nằm trong nhóm 3 lĩnh vực bị tấn công nhiều nhất, với trung bình hơn 4.600 cuộc tấn công mỗi tuần trong một số giai đoạn cao điểm, cao gấp đôi mức trung bình của các ngành kinh tế khác. Các nền tảng học trực tuyến trở thành mục tiêu "mềm" hấp dẫn đối với tội phạm mạng vì những lý do sau:

Một là: Khối lượng dữ liệu khổng lồ và nhạy cảm: Hệ thống lưu trữ thông tin cá nhân của hàng triệu học viên (họ tên, ngày sinh, số điện thoại, địa chỉ, số căn cước công dân, dữ liệu tài chính liên quan đến học phí, điểm số, bài tập, hồ sơ sức khỏe, hình ảnh cá nhân), cùng với tài liệu giảng dạy, đề thi, ngân hàng câu hỏi, và dữ liệu hành chính học đường. Dữ liệu này có giá trị cao trên thị trường đen.

Hai là: Hạ tầng bảo mật còn yếu và không đồng bộ: Nhiều cơ sở giáo dục vẫn sử dụng hệ thống cũ, thiếu các công cụ hiện đại như phát hiện và ứng phó điểm cuối, quản lý thông tin và sự kiện bảo mật, kiến trúc không tin cậy, hoặc chỉ triển khai tường lửa cơ bản mà không có chiến lược bảo mật toàn diện, giám sát liên tục, sao lưu dự phòng theo quy tắc 3-2-1.

Ba là: Yếu tố con người là lỗ hổng lớn nhất: Nhận thức bảo mật ở cả giảng viên và sinh viên còn rất thấp; tâm lý ngại báo cáo sự cố do sợ bị trách nhiệm hoặc không biết báo cáo ở đâu; thiếu kỹ năng nhận diện lừa đảo tinh vi (lừa đảo qua email, giả mạo sâu, kỹ thuật xã hội); và văn hóa "im lặng" khi xảy ra sự cố, làm mất "thời điểm vàng" để ứng cứu.

Bốn là: Tính chất tấn công ngày càng tinh vi: Tội phạm mạng sử dụng trí tuệ nhân tạo để tạo email lừa đảo cá nhân hóa, mã độc tự động lây lan, mã độc tống tiền mã hóa nhanh và tống tiền dữ liệu thay vì chỉ mã hóa tệp, hoặc tấn công chuỗi cung ứng qua các tiện ích mở rộng hệ thống quản lý học tập.

1.1. Các loại rủi ro chính trong đào tạo trực tuyến tại Việt Nam năm 2025

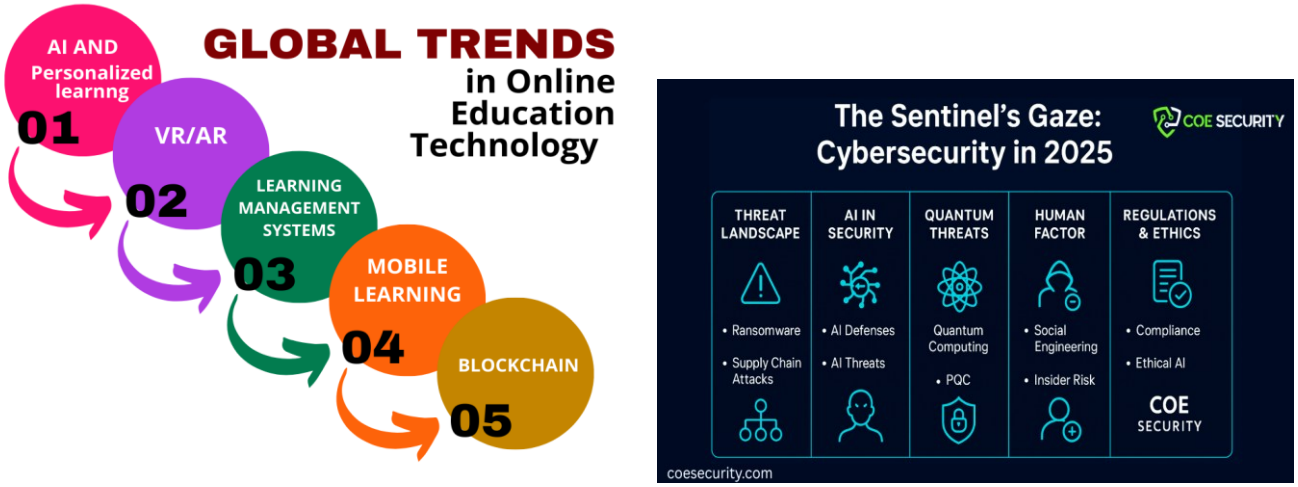
Lừa đảo qua email và kỹ thuật xã hội (chiếm tỷ lệ cao nhất 38-45%): Các hình thức lừa đảo qua email giả mạo "cập nhật điểm thi", "thông báo học bổng khẩn cấp", "mời tham gia hội thảo trực tuyến miễn phí", hoặc tin nhắn Zalo/Facebook từ tài khoản giả mạo giảng viên. Tấn công này khai thác sự thiếu cảnh giác, dẫn đến đánh cắp tài khoản học tập, truy cập trái phép vào hệ thống điểm, hoặc lây lan mã độc.

Mã độc tống tiền (25-32%, mức độ thiệt hại tăng mạnh): Mã hóa dữ liệu và đòi tiền chuộc, thường nhắm vào hệ thống quản lý học tập, kho tài liệu, hoặc cơ sở dữ liệu điểm thi. Các vụ điển hình năm 2025 gây gián đoạn học tập hàng tuần, mất dữ liệu không thể khôi phục nếu không có sao lưu.

Rò rỉ dữ liệu cá nhân (vi phạm nghiêm trọng

Nghị định số 13/2023/NĐ-CP): Hàng triệu tài khoản học viên bị lộ thông tin (tên, số điện thoại, email, điểm số), thường do lỗ hổng trong lưu trữ đám mây, quản lý tài khoản yếu, hoặc tấn công từ bên trong.

Tấn công từ chối dịch vụ (18–22%): Làm sập cổng thông tin tuyển sinh, nền tảng học trực tuyến trong các kỳ thi quan trọng, gây gián đoạn lớn và mất lòng tin [6].



(a) (b)

Hình 1. Tác động hai mặt của AI năm 2025

(a) Xu hướng toàn cầu trong công nghệ giáo dục trực tuyến năm 2025, nhấn mạnh AI và bảo mật

(b) Tổng quan các thách thức an ninh mạng năm 2025, bao gồm AI và mối đe dọa.

Nguồn dữ liệu: (a) http://coesecurity.com/ - (b) http://tinasoft.io

1.2. Để định lượng mức độ nghiêm trọng, bài báo áp dụng công thức rủi ro tổng hợp dựa trên Khung NIST

Công thức 1: Mức độ rủi ro tổng hợp

$$R = P \times I \times (1 - C) \quad (1)$$

Trong đó:

R: Mức độ rủi ro (điểm rủi ro, càng cao càng nguy hiểm).

P: Xác suất xảy ra ($0 \leq P \leq 1$).

I: Mức độ tác động (thang điểm 1–5: 1 = thấp, 5 = rất cao).

C: Hiệu quả kiểm soát hiện tại ($0 \leq C \leq 1$).

Ví dụ: minh họa cho tấn công mã độc tống tiền trong giáo dục Việt Nam năm 2025:

$P \approx 0.28$ (dựa trên tỷ lệ 25–32% các vụ tấn công).

$I = 5$ (rất cao: mất dữ liệu, gián đoạn học kỳ, thiệt hại kinh tế, mất uy tín).

$C \approx 0.25$ (thấp: chỉ có sao lưu thủ công, thiếu phát hiện và ứng phó điểm cuối, diễn tập chưa thường xuyên).

→ s (rủi ro cao, cần can thiệp khẩn cấp).

Nếu C tăng lên 0.60 nhờ diễn tập và sao lưu tốt, R giảm còn 0.56 (giảm 47%). Công thức này chứng minh rằng cải thiện kiểm soát (C) có tác động rất lớn đến việc giảm rủi ro.

Tiếp theo, xác suất xảy ra ít nhất một sự cố nghiêm trọng trong năm có thể được tính bằng mô hình Poisson:

Công thức 2: Xác suất xảy ra ít nhất một sự cố nghiêm trọng trong năm:

$$P(X \geq 1) = 1 - e^{(-\lambda t)} \quad (2)$$

Trong đó:

λ: Tần suất trung bình sự cố mỗi năm (dựa trên dữ liệu 2025, λ ≈ 228 cho giáo dục toàn cầu, điều chỉnh lên ≈ 280 cho Việt Nam do hạ tầng yếu hơn).t = 1 năm.

→ $\mathbf{P(X \geq 1) = 1 - e^{(-280)} \approx 1}$ (gần 100%).

Điều này cho thấy gần như chắc chắn một cơ sở giáo dục sẽ gặp ít nhất một sự cố nghiêm trọng trong năm nếu không có biện pháp can thiệp mạnh mẽ và liên tục.

Thời gian ứng phó trung bình tại Việt Nam

năm 2025 trong giáo dục ước tính 7–18 ngày, cao hơn nhiều so với chuẩn quốc tế (thường dưới 72 giờ) [7]. Phân tích chi tiết theo công thức:

Công thức 3: Thời gian ứng phó trung bình Thời gian ứng phó trung bình = Thời gian phát hiện trung bình + Thời gian thừa nhận trung bình + Thời gian cách ly trung bình + Thời gian khắc phục và phục hồi trung bình (3)

Giá trị điển hình tại Việt Nam 2025:

Thời gian phát hiện trung bình ≈ 28–45 giờ (thiếu công cụ phát hiện chủ động như phát hiện bất thường bằng trí tuệ nhân tạo, quản lý thông tin và sự kiện bảo mật).

Thời gian thừa nhận trung bình ≈ 4–12 giờ (ngại báo cáo).

Thời gian ứng phó trung bình ≈ 10–12 ngày, dẫn đến thiệt hại kinh tế lớn (ước tính hàng chục tỷ đồng mỗi vụ lớn), mất dữ liệu không thể khôi phục, và ảnh hưởng nghiêm trọng đến tiến độ học tập.

Những dữ liệu và công thức trên cho thấy thực trạng bảo mật trong đào tạo trực tuyến tại Việt Nam năm 2025 là cực kỳ nghiêm trọng, đòi hỏi các giải pháp toàn diện, không chỉ dừng ở kỹ thuật mà phải tập trung mạnh vào yếu tố con người, văn hóa tổ chức và phối hợp đa bên.

2. Cơ sở lý luận

Nghiên cứu sử dụng Khung an ninh mạng NIST CSF 2.0 (Khung An ninh mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia phiên bản 2.0, công bố năm 2024) làm nền tảng lý thuyết cốt lõi. Đây là khung quản trị an ninh mạng được công nhận rộng rãi trên toàn cầu, linh hoạt, có thể áp dụng cho mọi quy mô tổ chức từ doanh nghiệp nhỏ đến cơ quan nhà nước và cơ sở giáo dục.

Khung NIST bao gồm sáu chức năng chính, được thiết kế theo cách tiếp cận vòng đời liên tục:

Quản trị: Xây dựng chính sách, phân bổ nguồn lực, thiết lập cơ chế phối hợp, xác định vai trò trách nhiệm.

Nhận diện: Xác định tài sản, rủi ro, lỗ hổng, bối cảnh kinh doanh và mối đe dọa.

Bảo vệ: Triển khai các biện pháp phòng ngừa (tường lửa, mã hóa, quản lý truy cập, đào tạo nhận thức).

Phát hiện: Phát hiện sớm các sự kiện bất thường và sự cố (giám sát nhật ký, quản lý thông tin và sự kiện bảo mật, phát hiện xâm nhập).

Phản ứng: Ứng cứu, kiểm soát, phân tích và giảm thiểu tác động của sự cố.

Phục hồi: Khôi phục hệ thống, học hỏi từ sự cố, cải thiện liên tục.

Trong nghiên cứu này, trọng tâm được đặt vào ba chức năng chính:

Thứ nhất về nhận diện: Nhận diện và định lượng rủi ro, lập bản đồ lỗ hổng trong hệ thống đào tạo trực tuyến.

Thứ hai về phản ứng: Xây dựng quy trình ứng cứu nhanh chóng, hiệu quả, giảm thiểu thiệt hại.

Thứ ba là về quản trị: Thiết lập cơ chế phối hợp đa bên, phân định rõ trách nhiệm giữa Ban giám hiệu, phòng ban chức năng, giảng viên, sinh viên và nhân sự Công nghệ thông tin.

Khung NIST CSF 2.0 được lựa chọn vì những ưu điểm nổi bật:

Tính linh hoạt cao, phù hợp với các tổ chức giáo dục có nguồn lực hạn chế.

Đã được áp dụng thành công tại nhiều quốc gia (Hoa Kỳ, Singapore, Liên minh châu Âu) và được điều chỉnh theo bối cảnh địa phương.

Cung cấp ngôn ngữ chung để giao tiếp giữa lãnh đạo, kỹ thuật viên và người dùng cuối.

Hỗ trợ tích hợp các công cụ định lượng (rủi ro, thời gian ứng phó trung bình, hiệu quả kiểm soát) để đo lường tiến bộ [8].

2.1. Nghiên cứu bổ sung hai yếu tố quan trọng mà khung NIST chưa nhấn mạnh đủ:

Một là: Yếu tố con người, tâm lý ngại báo cáo, thiếu nhận thức, kỹ năng mềm - đây là nguyên nhân chính gây ra “khoảng trống an ninh” tại Việt Nam.

Hai là: Văn hóa bảo mật, Chuyển từ trạng thái “tĩnh” (có quy định nhưng không thực thi) sang trạng thái “động” (phản xạ có điều kiện) thông qua diễn tập định kỳ.

Để định lượng hiệu quả, nghiên cứu sử dụng các công thức toán học cơ bản và mở rộng:

Mức độ rủi ro tổng hợp (dựa trên Khung NIST

và mô hình rủi ro chuẩn):

$$R = P \times I \times (1 - C)$$

Ví dụ minh họa cho lừa đảo qua email:

$P \approx 0.40$ (xác suất cao do email giả mạo phổ biến).

$I = 4$ (tác động cao: đánh cắp tài khoản, lây lan mã độc).

$C \approx 0.20$ (kiểm soát thấp: ít đào tạo nhận thức). $\rightarrow R = 0.40 \times 4 \times 0.80 = 1.28$ (rủi ro cao). Nếu C tăng lên 0.60 qua đào tạo và diễn tập, R giảm còn 0.64 (giảm 50%).

Xác suất xảy ra ít nhất một sự cố nghiêm trọng trong năm (mô hình Poisson):

$$P(X \geq 1) = 1 - e\text{^}(-\lambda t)$$

Dữ liệu 2025: $\lambda \approx 280$ (tấn công nghiêm trọng/năm, điều chỉnh từ 228 toàn cầu).

$\rightarrow P(X \geq 1) \approx 1$ (gần chắc chắn xảy ra).

Thời gian ứng phó trung bình:

Thời gian ứng phó trung bình = Thời gian phát hiện trung bình + Thời gian thừa nhận trung bình + Thời gian cách ly trung bình + Thời gian khắc phục và phục hồi trung bình

Giá trị điển hình tại Việt Nam 2025:

Thời gian phát hiện trung bình ≈ 35 giờ.

Thời gian thừa nhận trung bình ≈ 8 giờ.

Thời gian cách ly trung bình ≈ 24 giờ. Thời gian khắc phục và phục hồi trung bình ≈ 7 ngày.

→ Thời gian ứng phó trung bình ≈ 9–10 ngày.

Xác suất thiệt hại nghiêm trọng nếu thời gian ứng phó vượt ngưỡng (mô hình logistic):

P(Thiệt hại nghiêm trọng | Thời gian ứng phó > ngưỡng) = $1 / (1 + e\text{^}(-\beta$(Thời gian ứng phó - ngưỡng)))

$\boldsymbol{\beta}$ = $\mathbf{0.25}$ (hệ số nhạy), ngưỡng = 72 giờ.

Thời gian ứng phó = 240 giờ (10 ngày): $\boldsymbol{P \approx 0.99}$ (rất cao).

Thời gian ứng phó = 48 giờ (sau cải thiện): $\boldsymbol{P \approx 0.20}$ (thấp).

Tỷ lệ báo cáo sau n lần diễn tập (mô hình logistic cải thiện):

$$R(n) = R_0 + (R_{\max} - R_0) \times (1 - e\text{^}(-\alpha n))$$

Giả sử R_0 = 0.18,$R_{\max}$ = 0.90,α = 0.22:

$n = 0$: 18%

$n = 4$: 62%

$n = 8$: 85%

$n = 10$: 89%

Giải thích tính toán R (ví dụ lừa đảo qua email): R = 0.40 × 4 × (1 - 0.20) = 1.28 (rủi ro cao).

Xác suất xảy ra ít nhất một sự cố nghiêm trọng: λ ≈ 280 → P(X ≥ 1) ≈ 1 (gần chắc chắn).

Thời gian ứng phó trung bình: Thời gian ứng phó trung bình ≈ 10–12 ngày, cao hơn chuẩn quốc tế 5–10 lần do thời gian thừa nhận và thời gian khắc phục lớn.

Bảng 1. Các loại rủi ro bảo mật phổ biến trong giáo dục

Loại rủi ro	Tỷ lệ ước tính (%)	Mức độ tác động (I)	Xác suất trung bình (P)	Rủi ro ước tính (R)	Thời gian ứng phó trung bình	Ví dụ thực tế tại Việt Nam
Lừa đảo qua email	38-45	4	0.40	1.28	4-12 giờ (thời gian thừa nhận cao)	Email giả mạo "cập nhật điểm thi", "học bổng"
Mã độc tống tiền	25-32	5	0.28	1.05	3-15 ngày (thời gian khắc phục cao)	Tấn công hệ thống quản lý học tập một số trường đại học lớn
Rò rỉ dữ liệu	Cao	5	0.35	1.31	5-10 ngày	Hàng triệu tài khoản học viên bị lộ thông tin
Tấn công từ chối dịch vụ	18s-22	3	0.20	0.48	12-48 giờ	Tấn công cổng thông tin tuyển sinh

Chú thích: Kết quả khảo sát và thống kê của tác giả, 2025

2.2. Mô hình phối hợp đa bên

Công thức 4: Hiệu quả phối hợp:

$$E = (w_1 \times w_2 \times w_3 \times w_4)^{(1/4)} \quad (4)$$

Ví dụ: Hiện tại w trung bình = 0.5 → E = 0.5 (thấp). Sau cải thiện w = 0.8 → E = 0.8 (cao).

2.3. Giải pháp định lượng

Giải pháp cốt lõi là tổ chức diễn tập sự cố định kỳ (4–6 lần/năm). Hiệu quả được đo bằng:

Công thức 5: Tỷ lệ báo cáo sau n lần diễn tập:

$$R(n) = R_0 + (R_{\max} - R_0) \times (1 - e^{(-\alpha n)}) \quad (5)$$

Tham số:

$R_0 = 0.18, R_{\max} = 0.90, \alpha = 0.22.$

Kết quả tính toán chi tiết:

$n = 0$: 18%

$n = 2$: 38% (*cải thiện* 20%)

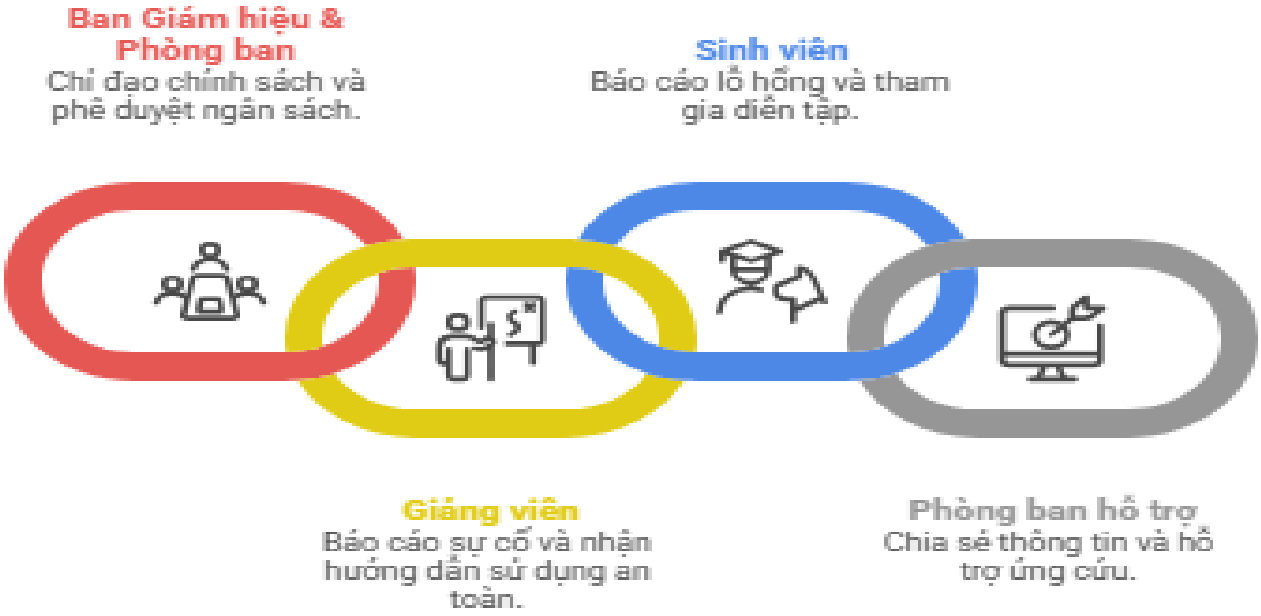
$n = 4$: 62% (*cải thiện* 44%)

$n = 6$: 78% (*cải thiện* 60%)

$n = 8$: 85% (*cải thiện* 67%)

$n = 10$: 89% (*cải thiện* 71%)

$n = 12$: 90% (đạt *mục tiêu*)



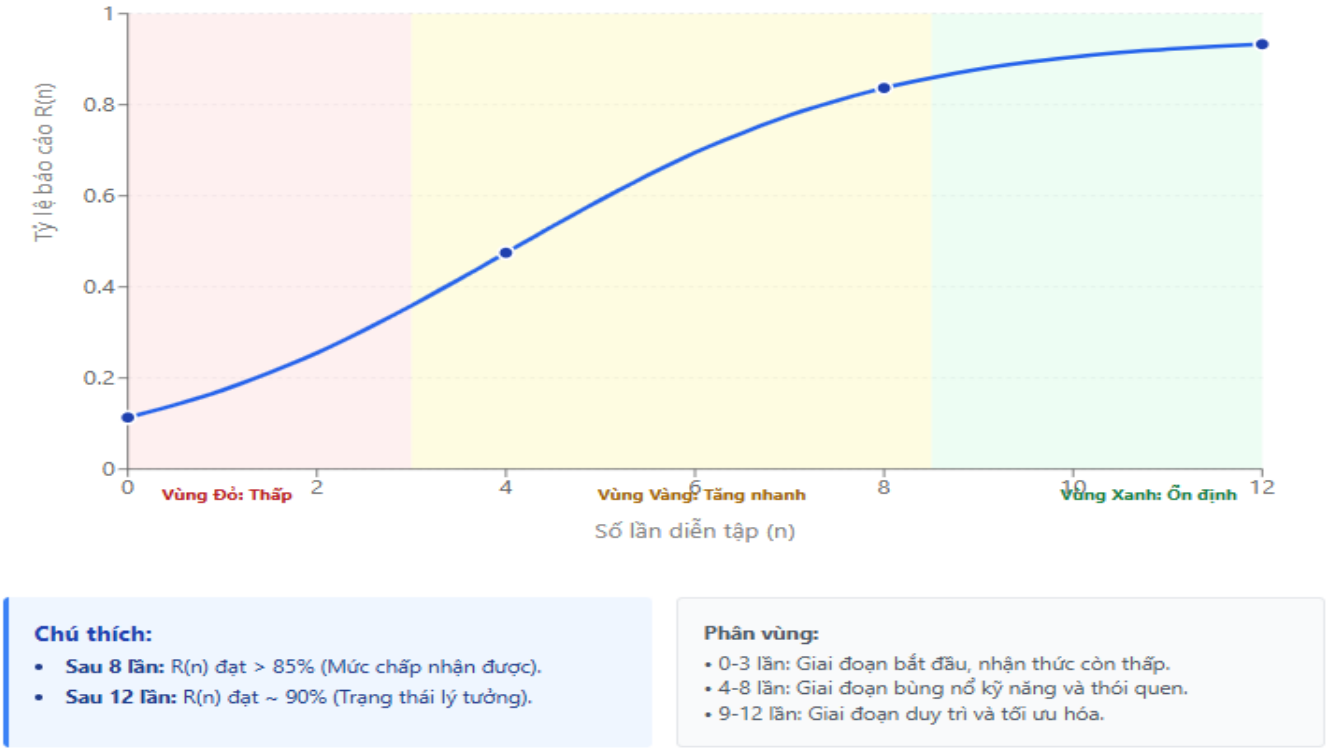
Hình 2. Mô hình phối hợp đa bên trong bảo mật giáo dục số

Chú thích: Nhóm tác giả tổng hợp

Bảng 2. Dự báo cải thiện tỷ lệ báo cáo theo số lần diễn tập

Số lần diễn tập (n)	Tỷ lệ báo cáo R(n) (%)	Cải thiện so với ban đầu (%)	Giai đoạn	Ghi chú đề xuất hành động
0	18	0	Ban đầu	Trạng thái hiện tại – rất thấp
2	38	20	Khởi động	Tập trung nâng nhận thức cơ bản
4	62	44	Tăng tốc	Tăng tần suất diễn tập, mở rộng đối tượng
6	78	60	Gần đạt yêu cầu	Đánh giá lại quy trình, điều chỉnh kịch bản
8	85	67	Đạt mức tốt	Khuyến nghị duy trì 4–6 lần/năm
10	89	71	Gần lý tưởng	Tập trung duy trì và mở rộng cho sinh viên
12	90	72	Ổn định	Đánh giá văn hóa bảo mật toàn tổ chức

Chú thích: Kết quả khảo sát và thống kê của tác giả, 2025



Hình 2. Mô hình phối hợp đa bên trong bảo mật giáo dục số

Chú thích: Kết quả khảo sát và thống kê của nhóm tác giả, 2025

Công thức 6: Xác suất thiệt hại nghiêm trọng nếu thời gian ứng phó vượt ngưỡng:

P(Thiệt hại nghiêm trọng | Thời gian ứng phó > ngưỡng) = 1 / (1 + e^(−β (Thời gian ứng phó − ngưỡng))) (6)

Tham số: $\beta = 0.25$, ngưỡng = 72 giờ.

Thời gian ứng phó = 240 giờ (10 ngày): $P \approx 0.99$ (rất cao).

Thời gian ứng phó = 48 giờ (sau cải thiện): $P \approx 0.20$ (thấp).

3. Kết luận và kiến nghị

3.1. Kết luận

Bảo mật dữ liệu trong đào tạo trực tuyến tại Việt Nam không chỉ là vấn đề kỹ thuật đơn thuần mà là một bài toán hệ thống phức tạp, liên quan chặt chẽ đến công nghệ, quy trình tổ chức và yếu tố con người. Thông qua phân tích định lượng bằng các công thức toán học, nghiên cứu đã chứng minh rõ ràng rằng:

Rủi ro gần như chắc chắn xảy ra nếu không có can thiệp mạnh mẽ và liên tục (xác suất xảy ra ít nhất một sự cố nghiêm trọng trong năm ≈ 100% theo mô hình Poisson).

Thời gian ứng phó trung bình hiện nay (khoảng 10-12 ngày) là quá cao, dẫn đến thiệt hại kinh tế, xã hội và uy tín nghiêm trọng, nhưng có thể giảm đáng kể xuống dưới 72 giờ thông qua cải thiện quy trình và diễn tập.

Diễn tập định kỳ có khả năng nâng tỷ lệ báo cáo từ 18% lên trên 85% chỉ sau 8-10 lần (theo mô hình logistic), từ đó tạo ra phản xạ "động" trong bảo mật thay vì trạng thái "tĩnh" (chỉ có quy định trên giấy mà không thực thi).

Xác suất thiệt hại nghiêm trọng giảm mạnh khi thời gian ứng phó được kiểm soát dưới ngưỡng 72 giờ (từ 99% xuống dưới 20% theo mô hình logistic).

Nhân sự Công nghệ thông tin cần được định vị lại với vai trò trung tâm điều phối - vừa làm chủ kỹ thuật (tường lửa, mạng riêng ảo, phát hiện bằng trí tuệ nhân tạo, ứng cứu sự cố), vừa dẫn dắt văn hóa bảo mật toàn tổ chức (thông qua diễn tập, hướng dẫn, tham mưu chính sách). Việc triển khai mô hình phối hợp đa bên, diễn tập định kỳ, chính sách "không trách phạt báo cáo sớm" và phân định rõ trách nhiệm của từng bên (Ban Giám hiệu, giảng

viên, sinh viên) là giải pháp thực tiễn, khả thi, có cơ sở khoa học và mang lại hiệu quả cao nhất [9]. Chỉ khi toàn bộ hệ sinh thái giáo dục cùng hành động đồng bộ, Việt Nam mới có thể xây dựng một hệ thống giáo dục số an toàn, bền vững, góp phần thực hiện thành công mục tiêu quốc gia trở thành quốc gia số vào năm 2030 và tầm nhìn phát triển đến năm 2045.

3.2. Kiến nghị chi tiết

- Đối với Ban Giám hiệu và các phòng ban chức năng:

Ban hành văn bản chính sách bảo mật toàn diện (Quyết định của Hiệu trưởng/Hội đồng trường), bao gồm: chính sách "không truy cứu trách nhiệm khi báo cáo sự cố sớm", quy định bắt buộc xác thực hai lớp, sao lưu dữ liệu theo quy tắc 3-2-1.

Phân bổ ngân sách ổn định: 8–15% ngân sách Công nghệ thông tin dành riêng cho bảo mật (phát hiện và ứng phó điểm cuối, quản lý thông tin và sự kiện bảo mật, diễn tập, đào tạo).

Thành lập và vận hành Nhóm ứng cứu sự cố: thành viên từ Công nghệ thông tin, Phòng Đào tạo, Phòng Hành chính, Ban Giám hiệu; họp định kỳ hàng quý để rà soát rủi ro, cập nhật kế hoạch ứng cứu.

Yêu cầu tất cả phòng ban tích hợp bảo mật vào quy trình: Phòng Đào tạo kiểm tra bảo mật trước khi triển khai nền tảng mới; Phòng Hành chính quản lý thu hồi tài khoản sinh viên tốt nghiệp kịp thời.

- Đối với Giảng viên:

Bảo vệ tài khoản cá nhân: Bật xác thực hai lớp cho email trường, Moodle, Zoom, Google Workspace; không dùng mật khẩu chung cho nhiều nền tảng.

Giám sát và hướng dẫn sinh viên: Trước mỗi buổi học trực tuyến, dành 2–3 phút nhắc nhở không click liên kết lạ, không chia sẻ tài khoản.

Báo cáo nhanh: Khi nhận email lạ, tệp đính kèm đáng ngờ → chụp màn hình, ghi thời gian, gửi ngay cho bộ phận Công nghệ thông tin (không chuyển tiếp email để tránh lây lan). Mục tiêu: báo cáo trong vòng 30 phút.

Tích hợp giáo dục bảo mật vào bài giảng: Dành 10–15 phút đầu học kỳ giới thiệu về lừa đảo qua email, mã độc tống tiền, giả mạo sâu;

Sao lưu tài liệu: Lưu trữ slide, bài giảng, đề thi trên đám mây an toàn với xác thực hai lớp, không chỉ trên máy cá nhân hoặc ổ đĩa di động.

- Đối với Sinh viên:

Bảo vệ tài khoản học tập: Bật xác thực hai lớp ngay khi nhận tài khoản trường; không chia sẻ mật khẩu với bạn bè, nhóm chat Zalo/Facebook.

Nhận diện và tránh lừa đảo: Không click liên kết trong email "trúng học bổng", "cập nhật hồ sơ", "xem điểm thi"; kiểm tra kỹ địa chỉ email gửi phải là @tentruong.edu.vn.

Báo cáo kịp thời: Khi nghi ngờ bị xâm nhập hoặc nhận email lạ → chụp màn hình, ghi thời gian, gửi ngay cho giảng viên chủ nhiệm hoặc đường dây nóng Công nghệ thông tin (không cố tự xử lý bằng phần mềm crack).

Tham gia diễn tập: Tham gia đầy đủ buổi diễn tập lừa đảo qua email giả lập, xem đó là cơ hội học hỏi thay vì "bị lừa".

Bảo vệ thiết bị cá nhân: Cài phần mềm diệt vi-rút (Bảo vệ Windows, Avast miễn phí), cập nhật hệ điều hành và trình duyệt thường xuyên.

Đối với nhân sự Công nghệ thông tin:

Đóng vai trò trung tâm điều phối: Tổ chức diễn tập định kỳ (4–6 lần/năm), xây dựng kênh giao tiếp khẩn cấp (đường dây nóng 24/7, hệ thống phiếu yêu cầu, nhóm Zalo nội bộ).

Giám sát và phát hiện sớm: Triển khai quản lý thông tin và sự kiện bảo mật, phân tích nhật ký, phát hiện bất thường (tăng đột biến truy cập, tệp lạ).

Tham mưu chính sách: Đề xuất cho Ban Giám hiệu các chính sách như "không trách phạt báo cáo sớm", đào tạo nhận thức định kỳ.

Xây dựng tài liệu dễ hiểu: Đồ họa thông tin, video ngắn (3–5 phút) về cách bật xác thực hai lớp, nhận diện lừa đảo qua email, quy trình báo cáo

Tài liệu tham khảo

[1] Bộ Chính trị. (2024). Nghị quyết 52-NQ/TW về phát triển khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia. Văn phòng

Trung ương Đảng, Hà Nội.
[2] Tinasoft. (2025). Online Education Technology: Vietnam's Breakthrough in 2025. Hà Nội, Tinasoft.
[3] Bộ Chính trị. (2025). Nghị quyết 29-NQ/TW về đổi mới giáo dục và đào tạo, Hà Nội: Văn phòng Trung ương Đảng.
[4] World Economic Forum. (2025). Global Cybersecurity Outlook 2025. World Economic Forum.
[5] Check Point Research. (2025). Cyber Attacks Decline, but Ransomware Jumps 46%. Check Point.
[6] S. K. Sood. (2025). Ensuring Data Security in eLearning: Challenges and Solutions. In Proc. IEEE Int. Conf. e-Learning Security.
[7] Cisco. (2025). Vietnam - 2025 Cisco Cybersecurity Readiness Index. Cisco.
[8] Q. Trinh. (2025). Cybersecurity Profile 2025: Vietnam. University of Washington.
[9] M. A. A.-G. e. al. Best Practices for Ensuring Security and Privacy in E-Learning Platforms. IEEE Access, vol. 12, p. 12345-12360, 20