BẢO MẬT DỮ LIỆU TRONG THỜI ĐẠI CHUYỂN ĐỔI SỐ: VẤN ĐỀ VÀ GIẢI PHÁP

● **VŨ VĂN ĐIỆP**

Khoa Thương Mại, Trường Đại học Công Thương Thành phố Hồ Chí Minh

Email: diepvv@huit.edu.vn

TÓM TẮT:

Chuyển đổi số đang trở thành xu hướng tất yếu của các doanh nghiệp và tổ chức trên toàn cầu. Tuy nhiên, quá trình này đi kèm với nhiều rủi ro liên quan đến an toàn dữ liệu, bao gồm tấn công mạng, rò rỉ thông tin và sự thiếu hụt nhân lực an ninh mạng. Bài báo này phân tích thực trạng bảo mật dữ liệu trong bối cảnh chuyển đổi số, những thách thức mà các tổ chức đang phải đối mặt, đồng thời đề xuất một số giải pháp nhằm tăng cường bảo mật dữ liệu, bao gồm đầu tư vào hạ tầng an ninh mạng, đào tạo nhân sự, áp dụng công nghệ mới và xây dựng chính sách bảo mật chặt chẽ.

Từ khóa: chuyển đổi số, bảo mật dữ liệu.

1. Đặt vấn đề

Trong kỷ nguyên số hóa, dữ liệu đã trở thành tài sản vô giá đối với các doanh nghiệp và tổ chức. Theo IBM Security (2023), chi phí trung bình cho một vụ vi phạm dữ liệu đã tăng lên đến 4,45 triệu USD, cao hơn 15% so với ba năm trước. Điều này làm nổi bật tầm quan trọng của việc bảo vệ dữ liệu trước những mối đe dọa ngày càng gia tăng. Sự phát triển mạnh mẽ của các công nghệ như điện toán đám mây, Internet of Things (IoT), trí tuệ nhân tạo (AI) và dữ liệu lớn (Big Data) đã mang lại vô vàn lợi ích, nhưng cũng đồng thời đặt ra những thách thức bảo mật nghiêm trọng. Các cuộc tấn công mạng không chỉ nhằm vào các cá nhân mà còn nhắm đến các hệ thống quan trọng như chính phủ, ngân hàng, bệnh viện và các tập đoàn lớn, khiến việc bảo vệ dữ liệu trở thành ưu tiên hàng đầu trong chiến lược an ninh mạng của mọi tổ chức.

2. Thực trạng bảo mật dữ liệu trong thời đại chuyển đổi số

2.1. Bối cảnh bảo mật dữ liệu trên thế giới

Bảo mật dữ liệu là vấn đề quan trọng hàng đầu đối với các doanh nghiệp và tổ chức trên toàn cầu. Theo Verizon (2023), 94% các cuộc tấn công mạng có chủ đích, trong đó ransomware là hình thức tấn công phổ biến nhất. Báo cáo của Cybersecurity Ventures (2024) cho thấy hơn 60% các vụ rò rỉ dữ

liệu bắt nguồn từ lỗi con người hoặc hệ thống bảo mật không được cập nhật thường xuyên. Một vấn đề đáng lo ngại khác là sự thiếu hụt nhân lực an ninh mạng. Theo ISC² (2024), thế giới đang thiếu khoảng 3,4 triệu chuyên gia bảo mật, dẫn đến khó khăn trong việc bảo vệ dữ liệu. Các vụ tấn công mạng lớn như vụ Colonial Pipeline (Mỹ, 2021), hệ thống ngân hàng châu Âu và dữ liệu y tế NHS (Anh, 2023) là minh chứng rõ ràng cho sự nguy hiểm của các cuộc tấn công mạng trên phạm vi toàn cầu.

2.2. Tình hình bảo mật dữ liệu tại Việt Nam

Tại Việt Nam, tình trạng bảo mật dữ liệu cũng đáng báo động. Theo Bộ Thông tin và Truyền thông (2023), chỉ riêng trong năm 2023 đã có 13.900 cuộc tấn công mạng vào các hệ thống thông tin quan trọng. Báo cáo từ NCSC Việt Nam (2024) chỉ ra rằng các cuộc tấn công phishing, ransomware và DDoS đang gia tăng mạnh mẽ, đặc biệt trong các lĩnh vực tài chính, thương mại điện tử và chính phủ điện tử. Một nghiên cứu của PwC (2024) cho thấy hơn 70% doanh nghiệp vừa và nhỏ (SMEs) tại Việt Nam không có bộ phận chuyên trách về an ninh mạng, khiến họ trở thành mục tiêu dễ bị tấn công.

Số liệu thống kê từ Trung tâm Viễn thông Khu Công viên phần mềm Quang Trung (2024) cho thấy, trong khoảng 6 tháng đầu năm 2024, có hơn 5.000 vụ tấn công mạng vào các hệ thống tại Việt Nam, tăng khoảng 40% so với cùng kỳ năm 2023. Các vụ tấn công có chủ đích vào các cơ sở trọng yếu cũng tăng khoảng 9% so với cùng kỳ năm 2023. Những cơ sở này bao gồm các tổ chức tài chính, cơ quan chính phủ và các doanh nghiệp lớn, thường là mục tiêu do lưu trữ nhiều dữ liệu quan trọng. Các hình thức tấn công chính bao gồm tấn công người dùng thông qua email giả mạo và khai thác lỗ hổng phần mềm. Đặc biệt, có gần 400 website của các cơ quan nhà nước và tổ chức giáo dục bị hacker tấn công, chèn mã quảng cáo cờ bạc, cá độ. Điều này không chỉ gây ra rủi ro về mất mát dữ liệu mà còn có thể phát tán mã độc và các nội dung xấu.

3. Những thách thức trong bảo mật dữ liệu

3.1. Sự gia tăng của tấn công mạng có chủ đích

Các cuộc tấn công mạng có chủ đích ngày càng tinh vi và khó phát hiện. Theo Verizon (2023), ransomware chiếm 62% tổng số các cuộc tấn công mạng trong năm 2023. Phương thức này mã hóa dữ liệu của nạn nhân và yêu cầu tiền chuộc để mở khóa, gây thiệt hại lớn về tài chính. Các cuộc tấn công phishing cũng gia tăng, với 91% các vụ tấn công mạng bắt đầu từ email lừa đảo (IBM Security, 2023). Ngoài ra, 1.500 vụ tấn công DDoS vào hệ thống ngân hàng và doanh nghiệp tại Việt Nam trong năm 2023 (NCSC Việt Nam, 2024) cho thấy tội phạm mạng đang tận dụng mọi lỗ hổng để gây thiệt hại.

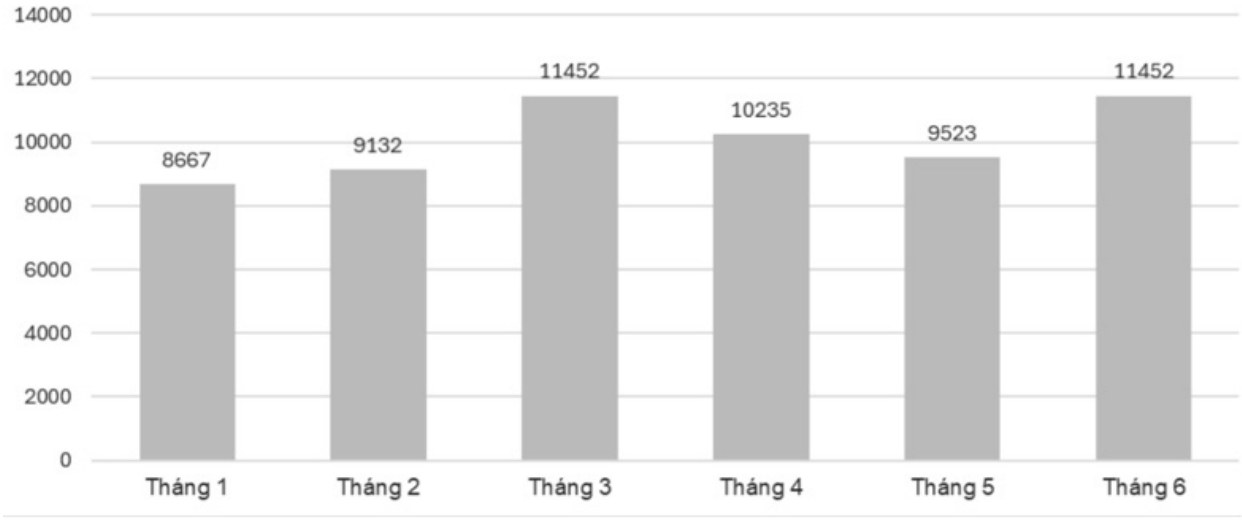
Lừa đảo trực tuyến tại Việt Nam đang có xu hướng gia tăng cả về mức độ tinh vi lẫn quy mô. Theo thông tin từ Cục An toàn thông tin (ATTT) thuộc Bộ Thông tin và Truyền thông (TT&TT), trong 9 tháng đầu năm 2024, hơn 22.200 phản ánh về các vụ lừa đảo trực tuyến đã được gửi đến Cổng cảnh báo an toàn thông tin Việt Nam. Trong đó, hơn 80% các vụ lừa đảo có liên quan đến việc chiếm đoạt tài sản, thông qua các hình thức lừa đảo kỹ thuật số như giả mạo ngân hàng, ví điện tử và các trò lừa đảo đầu tư. Đặc biệt, 70% các vụ lừa đảo trực tuyến xảy ra trên các nền tảng mạng xã hội như Zalo và Facebook.

Tháng 6/2024 ghi nhận số lượng báo cáo cao nhất trong quý 2, lên đến 11.452 vụ, cho thấy sự gia tăng mạnh mẽ về tình hình an ninh mạng và các hành vi lừa đảo. Mức độ gia tăng này có thể được tác động bởi Quyết định số 2345/QĐ-NHNN của Ngân hàng Nhà nước, có hiệu lực từ ngày 1/7/2024, liên quan đến các giải pháp bảo mật như sinh trắc học cho các giao dịch thanh toán trực tuyến và thẻ ngân hàng (Hình1).

3.2. Quản lý dữ liệu phi tập trung và rủi ro từ điện toán đám mây

Với sự phát triển mạnh mẽ của điện toán đám mây và IoT, dữ liệu doanh nghiệp không còn được lưu trữ tập trung mà bị phân tán trên nhiều nền tảng. Điều này tạo ra các lỗ hổng bảo mật nghiêm trọng nếu không có biện pháp kiểm soát chặt chẽ. Theo McAfee (2023), 40% doanh nghiệp không mã hóa dữ liệu lưu trữ trên đám mây, làm tăng nguy cơ rò rỉ thông tin. Đồng thời, báo cáo của Kaspersky (2023) cho thấy hơn 1,5 tỷ thiết bị IoT đã bị tấn công chỉ trong năm 2023.

Hình 1: Báo cáo về lừa đảo qua mạng tại Việt Nam năm 2024



Nguồn: https://chongluadao.vn/.

3.3. Thiếu hụt nhân sự an ninh mạng

Bảo mật dữ liệu không chỉ đòi hỏi công nghệ tiên tiến mà còn cần đội ngũ chuyên gia có kinh nghiệm. Tuy nhiên, theo ISC² (2024), thế giới hiện đang thiếu 3,4 triệu chuyên gia bảo mật, trong đó Việt Nam thiếu hơn 50.000 chuyên gia an ninh mạng (Bkav, 2023).

Theo khảo sát của Hiệp hội An ninh mạng quốc gia, hơn 20% các cơ quan và doanh nghiệp tại Việt Nam chưa có nhân sự chuyên trách về an ninh mạng, trong khi 35,56% các đơn vị không đáp ứng đủ số lượng nhân sự cần thiết cho công tác bảo mật và an ninh mạng, dự kiến sẽ thiếu hụt khoảng 700.000 nhân sự chuyên trách về an ninh mạng trong thời gian tới. Điều này phản ánh sự thiếu hụt nhân lực trong lĩnh vực an ninh mạng, trong khi nhu cầu bảo vệ hệ thống thông tin, dữ liệu và cơ sở hạ tầng quan trọng ngày càng gia tăng. Việc thiếu hụt nhân sự chuyên môn có thể gây khó khăn cho các cơ quan, doanh nghiệp trong việc đối phó với các mối đe dọa an ninh mạng, từ các cuộc tấn công có chủ đích đến các mối nguy hiểm tiềm tàng khác.

3.4. Nhận thức và tuân thủ bảo mật còn thấp

Sự hạn chế trong nhận thức về an toàn thông tin của nhiều tổ chức và cá nhân đã dẫn đến việc lơ là các biện pháp bảo vệ dữ liệu, khiến họ trở thành mục tiêu dễ bị lừa đảo và tấn công trên môi trường mạng. Nhiều doanh nghiệp chưa có chiến lược bảo mật rõ ràng, điều này tạo điều kiện cho tin tặc khai thác lỗ hổng. Theo PwC (2024), 45% doanh nghiệp chưa triển khai chính sách bảo mật dữ liệu toàn diện. Bên cạnh đó, 70% nhân viên sử dụng mật khẩu yếu hoặc trùng lặp, làm tăng nguy cơ bị tấn công (LastPass, 2023).

4. Giải pháp bảo mật dữ liệu trong chuyển đổi số

4.1. Đối phó với sự gia tăng của tấn công mạng có chủ đích

Phòng ngừa qua đào tạo: Một trong những biện pháp quan trọng trong công tác bảo mật là nâng cao nhận thức cho nhân viên về các nguy cơ bảo mật, đặc biệt là các cuộc tấn công phishing. Việc tổ chức các khóa đào tạo định kỳ sẽ giúp nhân viên nhận diện được các email lừa đảo và các hình thức tấn công khác, từ đó giảm thiểu khả năng bị tấn công. Chương trình đào tạo bảo mật cần được thiết kế một cách bài bản, bao gồm các tình huống thực tế và các phương pháp phòng tránh, giúp nâng cao ý thức bảo mật trong toàn bộ tổ chức.

Áp dụng bảo mật tầng sâu: Doanh nghiệp cần triển khai các biện pháp bảo mật nhiều lớp để bảo vệ

hệ thống khỏi các mối đe dọa từ nhiều hướng khác nhau. Các biện pháp này bao gồm sử dụng phần mềm chống vi-rút để phát hiện và ngăn chặn mã độc, thiết lập firewall để kiểm soát lưu lượng mạng và ngăn chặn các truy cập trái phép, cùng với việc triển khai hệ thống giám sát xâm nhập để phát hiện và phản ứng kịp thời với các hoạt động bất thường. Việc áp dụng bảo mật đa lớp không chỉ giúp giảm thiểu rủi ro mà còn tăng cường khả năng phòng thủ của doanh nghiệp trước các cuộc tấn công tinh vi.

Sử dụng công nghệ bảo mật nâng cao: Doanh nghiệp cần áp dụng các công nghệ bảo mật tiên tiến để phòng chống các mối đe dọa như ransomware. Điều này bao gồm việc sử dụng phần mềm bảo vệ chuyên biệt được thiết kế để phát hiện và ngăn chặn các cuộc tấn công ransomware, cũng như triển khai hệ thống giám sát để theo dõi và phát hiện sớm các dấu hiệu bất thường có thể là chỉ báo của một cuộc tấn công ransomware. Các biện pháp này giúp giảm thiểu khả năng bị tấn công và bảo vệ dữ liệu của doanh nghiệp khỏi những thiệt hại lớn do mã độc tống tiền gây ra.

4.2. Quản lý dữ liệu phi tập trung và rủi ro từ điện toán đám mây

Mã hóa dữ liệu đám mây: Trước khi lưu trữ dữ liệu trên các nền tảng điện toán đám mây, các tổ chức nên thực hiện mã hóa toàn bộ dữ liệu nhằm đảm bảo an toàn, bảo mật thông tin. Việc mã hóa sẽ giúp dữ liệu không thể bị đọc hoặc khai thác, ngay cả trong trường hợp hệ thống đám mây bị tấn công hoặc rò rỉ. Ngoài ra, các tổ chức cũng nên lựa chọn các nhà cung cấp dịch vụ đám mây uy tín, hỗ trợ các chuẩn mã hóa tiên tiến, đồng thời kết hợp sử dụng các khóa mã hóa riêng biệt để tăng cường khả năng kiểm soát và bảo vệ dữ liệu.

Kiểm soát quyền truy cập: Doanh nghiệp cần thiết lập một chính sách quản lý quyền truy cập nghiêm ngặt, đảm bảo rằng chỉ những cá nhân có thẩm quyền và đúng vai trò mới có quyền truy cập vào dữ liệu nhạy cảm. Việc áp dụng phương pháp xác thực đa yếu tố (MFA) sẽ gia tăng lớp bảo vệ, hạn chế tối đa nguy cơ bị truy cập trái phép, ngay cả khi thông tin tài khoản bị lộ. Bên cạnh đó, tổ chức nên thường xuyên rà soát, cập nhật và thu hồi quyền truy cập của những nhân sự không còn liên quan, nhằm đảm bảo hệ thống luôn được kiểm soát an toàn.

Đánh giá và giám sát các nhà cung cấp dịch vụ đám mây: Doanh nghiệp nên tiến hành đánh giá định kỳ các nhà cung cấp dịch vụ đám mây nhằm đảm bảo họ tuân thủ các tiêu chuẩn bảo mật quốc tế, có chính sách bảo vệ dữ liệu rõ ràng và biện pháp ứng phó sự cố hiệu quả. Ngoài ra, việc ký kết các thỏa thuận mức độ dịch vụ (SLA) chi tiết và theo dõi sát sao quá trình vận hành sẽ giúp doanh nghiệp giảm thiểu rủi ro và duy trì an toàn cho dữ liệu trong suốt quá trình sử dụng dịch vụ.

4.3. Thiếu hụt nhân sự an ninh mạng

Đào tạo và phát triển nhân lực: Doanh nghiệp cần đầu tư vào đào tạo nhân viên về bảo mật mạng. Các chương trình đào tạo có thể giúp nâng cao nhận thức và kỹ năng của đội ngũ nhân viên, từ đó giúp giảm thiểu các lỗ hổng bảo mật. Hơn nữa, việc hợp tác với các tổ chức đào tạo chuyên nghiệp hoặc cung cấp các khóa học về an ninh mạng sẽ giúp tăng cường khả năng phòng thủ.

Tuyển dụng chuyên gia an ninh mạng: Các doanh nghiệp cần tích cực tìm kiếm và thu hút các chuyên gia về an ninh mạng. Việc này đòi hỏi các chính sách đãi ngộ hấp dẫn và môi trường làm việc chuyên nghiệp để giữ chân những người có năng lực.

Tận dụng công nghệ tự động hóa: Áp dụng các công cụ và phần mềm bảo mật tự động giúp giảm thiểu gánh nặng công việc cho các chuyên gia bảo mật. Các công cụ như SIEM (Security Information and Event Management) hay EDR (Endpoint Detection and Response) sẽ giúp phát hiện và phản ứng nhanh chóng trước các mối đe dọa mà không cần sự can thiệp của con người.

4.4. Nhận thức và tuân thủ bảo mật còn thấp

Xây dựng chính sách bảo mật rõ ràng: Mỗi doanh nghiệp cần thiết lập một chính sách bảo mật dữ liệu chi tiết, cụ thể và được rà soát, cập nhật định kỳ để phù hợp với tình hình thực tế và các mối đe dọa mới. Chính sách này nên quy định rõ các quy trình bảo mật, tiêu chuẩn đặt và quản lý mật khẩu, yêu cầu bảo mật khi truy cập vào hệ thống, cách thức xử lý khi phát hiện sự cố an ninh, cũng như nguyên tắc trong việc lưu trữ, chia sẻ và bảo vệ dữ liệu nhạy cảm. Ngoài ra, doanh nghiệp nên tổ chức đào tạo định kỳ

để nhân viên hiểu rõ, tuân thủ và áp dụng nghiêm túc các chính sách này trong công việc hàng ngày.

Khuyến khích tuân thủ bảo mật: Doanh nghiệp cần xây dựng một văn hóa bảo mật mạnh mẽ, nơi mỗi nhân viên đều ý thức được vai trò và trách nhiệm của mình trong việc bảo vệ dữ liệu. Để thúc đẩy điều này, tổ chức có thể áp dụng các chương trình đào tạo định kỳ, lồng ghép nội dung bảo mật vào quy trình làm việc hằng ngày và khen thưởng những cá nhân, tập thể có ý thức tuân thủ tốt các quy định bảo mật. Bên cạnh đó, cần áp dụng các biện pháp xử lý kỷ luật rõ ràng đối với các trường hợp vi phạm, qua đó nâng cao tính răn đe và khuyến khích toàn bộ nhân viên nghiêm túc tuân thủ quy trình bảo mật dữ liệu.

Sử dụng các công cụ bảo mật hiện đại: Các tổ chức nên triển khai các công cụ quản lý mật khẩu, mã hóa dữ liệu và quản lý quyền truy cập để đảm bảo tuân thủ các tiêu chuẩn bảo mật, đồng thời tăng cường khả năng kiểm soát và phát hiện sớm các mối đe dọa. Bên cạnh đó, việc áp dụng các hệ thống giám sát an ninh mạng theo thời gian thực (SIEM), công nghệ bảo vệ điểm cuối (Endpoint Protection) và giải pháp xác thực đa yếu tố (MFA) sẽ giúp giảm thiểu nguy cơ bị tấn công, nâng cao độ an toàn cho hệ thống và dữ liệu.

5. Kết luận

Trong kỷ nguyên chuyển đổi số, bảo mật dữ liệu đóng vai trò then chốt trong việc đảm bảo sự phát triển bền vững của các doanh nghiệp và tổ chức. Cùng với những cơ hội mà chuyển đổi số mang lại, các rủi ro liên quan đến tấn công mạng, rò rỉ thông tin và sự thiếu hụt nhân lực an ninh mạng ngày càng trở nên phức tạp và khó lường. Do đó, các tổ chức cần chủ động triển khai các biện pháp toàn diện như đầu tư vào hạ tầng an ninh mạng, nâng cao nhận thức và kỹ năng của nhân viên, ứng dụng công nghệ tiên tiến và xây dựng chính sách bảo mật chặt chẽ. Chỉ khi có sự phối hợp đồng bộ giữa con người, công nghệ và quy trình, các tổ chức mới có thể tạo ra một môi trường số an toàn, sẵn sàng đón nhận và khai thác tối đa những giá trị mà chuyển đổi số mang lại■

TÀI LIỆU THAM KHẢO:

Tiếng Việt

Báo Hưng Yên. (n.d.). An ninh mạng Việt Nam đạt thành tựu lớn, nhưng tỷ lệ lừa đảo vẫn gia tăng. Truy cập tại https://baohungyen.vn/an-ninh-mang-viet-nam-dat-thanh-tuu-lon-nhung-ty-le-lua-dao-van-gia-tang-3175546.html

Chống Lừa Đảo. (2024, July). Tình trạng lừa đảo tại Việt Nam trong 6 tháng đầu năm 2023. Truy cập tại https://chongluadao.vn/blog/2024/07/tinh-trang-lua-dao-tai-viet-nam-trong-6-thang-dau-nam-2023/

Bkav. (2023). Cybersecurity Threats in Vietnam: A Growing Concern.

Tiếng Anh

Cybersecurity Ventures. (2023). Global Cybersecurity Market Size & Growth 2023. Available at https://cybersecurityventures.com/global-cybersecurity-market-size-growth-2023/

Cybersecurity Ventures. (2024). Cybersecurity Workforce Study 2024. Available at https://cybersecurityventures.com/cybersecurity-workforce-study-2024/

IBM Security. (2023). Cost of a data breach report 2023. Available at https://www.ibm.com/security/data-breach

ISC². (2024). Cybersecurity Workforce Gap 2024. Kaspersky. (2023). The State of IoT Security 2023.

LastPass. (2023). The Impact of Weak Passwords on Data Security. Available at https://www.lastpass.com/blog/weak-passwords-impact-data-security

McAfee. (2023). Cloud Security: Risks and Best Practices. Available at https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cloud-security-risks-and-best-practices.pdf

National Cyber Security Center (NCSC) Vietnam. (2024). Annual cybersecurity report 2024. National Cyber Security Center, Vietnam. Available at https://www.ncsc.gov.vn/en/reports/annual-cybersecurity-report-2024

PwC. (2024). Cybersecurity in the Digital Age: Trends and Challenges. https://www.pwc.com/gx/en/services/consulting/cybersecurity-in-the-digital-age-2024.html

PwC. (2024). The State of Cybersecurity in Small and Medium Businesses. Available at https://www.pwc.com/gx/en/services/consulting/state-of-cybersecurity-small-medium-businesses-2024.html

Verizon. (2023). 2023 Data Breach Investigations Report.

Ngày nhận bài: 24/2/2025
Ngày phản biện đánh giá và sửa chữa: 12/3/2025
Ngày chấp nhận đăng bài: 25/3/2025

DATA SECURITY IN THE DIGITAL TRANSFORMATION ERA: PROBLEMS AND SOLUTIONS

● **VU VAN DIEP**

Faculty of Commerce, Ho Chi Minh City University of Industry and Trade

ABSTRACT:

Digital transformation is an essential trend for businesses and organizations globally, yet it introduces substantial risks related to data security, including cyberattacks, data breaches, and a shortage of cybersecurity professionals. This study examines the current state of data security in the context of digital transformation, identifies the key challenges organizations face, and proposes effective solutions to strengthen data protection. These solutions encompass investing in cybersecurity infrastructure, enhancing workforce training, adopting cutting-edge technologies, and implementing stringent security policies.

Keywords: digital transformation, data security.