p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

THỰC TRẠNG VĂN HÓA AN TOÀN THÔNG TIN KẾ TOÁN CỦA CÁC DOANH NGHIỆP MAY MẶC TRÊN ĐỊA BÀN TỈNH THANH HÓA

Đặng Lan Anh[1], Lê Thị Oanh[2], Hoàng Thị Ngọc[2], Phạm Hùng Anh[3]

TÓM TẮT

Nghiên cứu này nhấn mạnh vai trò quan trọng và đánh giá thực trạng của văn hóa an toàn thông tin (VHATTT) trong việc bảo mật thông tin kế toán tại các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa. Trong bối cảnh số hóa, doanh nghiệp đối diện với nhiều rủi ro an ninh mạng nhưng mức độ nhận thức và thực hành các biện pháp bảo mật trong kế toán còn chưa tương xứng với yêu cầu thực tiễn. Nghiên cứu sử dụng phương pháp định tính và định lượng với mẫu khảo sát 326 nhà quản lý và nhân viên kế toán tại 287 doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa. Kết quả cho thấy những ưu điểm và hạn chế của văn hóa an toàn thông tin thông qua 4 yếu tố: nhận thức, hành vi, cam kết của lãnh đạo và đào tạo. Từ đó, nghiên cứu đề xuất những kiến nghị góp phần xây dựng, duy trì và tăng cường văn hóa an toàn thông tin kế toán trong các doanh nghiệp này.

Từ khóa: *Văn hóa an toàn thông tin, doanh nghiệp may mặc, Thanh Hóa.*

DOI: *https://doi.org/10.70117/hdujs.78.7.2025.807*

1. ĐẶT VẤN ĐỀ

Thông tin kế toán đóng vai trò vô cùng quan trọng trong quản lý và điều hành hoạt động kinh doanh của các doanh nghiệp. Tuy nhiên, trong thời đại số hóa mạnh mẽ, thông tin kế toán cũng đang đối diện với nhiều nguy cơ về bảo mật, từ việc mất mát dữ liệu, truy cập trái phép, đến các cuộc tấn công mạng phức tạp. Các cuộc tấn công mạng vào hệ thống thông tin kế toán còn ảnh hưởng đến uy tín, gây ra thiệt hại tài chính nghiêm trọng. Văn hóa an toàn thông tin (VHATTT) nói chung và VHATTT kế toán nói riêng đã thu hút sự quan tâm của nhiều nhà nghiên cứu và tổ chức lớn, đặc biệt trong bối cảnh các vụ tấn công mạng ngày càng gia tăng. Các nghiên cứu tập trung vào tác động của VHATTT đối với bảo mật dữ liệu tài chính và kế toán trong doanh nghiệp (PwC, KPMG, EY…), cũng như nhận thức và hành vi của nhân viên kế toán đối với an toàn thông tin, cho thấy yếu tố con người đóng vai trò quan trọng bên cạnh các giải pháp công nghệ; chính sách và khung pháp lý quốc tế trong việc bảo vệ dữ liệu kế toán (ví dụ: GDPR của EU, SOX của Mỹ); ứng dụng công nghệ bảo mật trong kế toán tài chính, như blockchain, AI trong phát hiện gian lận tài chính [10][18]. Các nghiên cứu chỉ ra rằng, một VHATTT mạnh giúp giảm thiểu rủi ro gian lận, thất thoát dữ liệu và tăng cường lòng tin của nhà đầu tư. Ở Việt Nam, VHATTT trong kế toán chưa

[1] *Khoa Kinh tế - Quản trị kinh doanh, Trường Đại học Hồng Đức; Email: danglananh@hdu.edu.vn*
[2] *Sinh viên Lớp K25D Đại học Kế toán, Khoa Kinh tế - Quản trị kinh doanh, Trường Đại học Hồng Đức*
[3] *Sinh viên Lớp K25C Đại học Kế toán, Khoa Kinh tế - Quản trị kinh doanh, Trường Đại học Hồng Đức*

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

nhận được nhiều sự quan tâm như trên thế giới, nhưng các nghiên cứu trong những năm gần đây đang dần tăng lên, tập trung vào nhận thức của kế toán viên và lãnh đạo doanh nghiệp về an toàn thông tin (chủ yếu là các doanh nghiệp vừa và nhỏ, nơi hệ thống bảo mật còn yếu); tác động của chuyển đổi số và việc ứng dụng phần mềm kế toán đến bảo mật thông tin; thực trạng và giải pháp nâng cao VHATTT trong kế toán doanh nghiệp; những rủi ro bảo mật khi sử dụng phần mềm kế toán phổ biến như MISA, FAST, và các hệ thống ERP [4]. Theo thống kê, nhiều cuộc tấn công mạng đã nhắm vào các doanh nghiệp vừa và nhỏ vì những doanh nghiệp này thường không có đủ nguồn lực để đầu tư vào các giải pháp bảo mật hiệu quả [5]. Do đó, văn hóa an toàn thông tin (VHATTT) trở thành một trong những ưu tiên hàng đầu trong lĩnh vực nghiên cứu và thực tiễn tại các doanh nghiệp.

Ngày 27/02/2023, Thủ tướng Chính phủ đã ban hành Quyết định số 153/QĐ-TTg phê duyệt "Quy hoạch tỉnh Thanh Hóa thời kỳ 2021- 2030 tầm nhìn đến năm 2045". Trong đó, chỉ rõ 06 lĩnh vực ưu tiên tạo sự phát triển đột phá cho phát triển kinh tế - xã hội tỉnh nhà. Trong đó, may mặc là một trong những ngành công nghiệp có giá trị lớn, năng suất cao, thu hút nhiều lao động sẽ được tập trung ưu tiên phát triển. Tỉnh Thanh Hóa hiện có 287 doanh nghiệp may mặc, tạo việc làm cho khoảng 150.000 lao động. Trong những năm gần đây, các doanh nghiệp may mặc đã đóng vai trò quan trọng trong tăng trưởng công nghiệp tỉnh Thanh Hóa. Trong năm 2024, các doanh nghiệp dệt may tại Thanh Hóa đã sản xuất hơn 700 triệu sản phẩm, tăng trưởng khoảng 20% so với năm trước. Trong tháng 1/2025, tổng giá trị xuất khẩu hàng hóa của Thanh Hóa ước đạt hơn 1 tỷ USD, tăng 30,94% so với cùng kỳ năm trước. Tuy nhiên, các doanh nghiệp may mặc tại tỉnh Thanh Hóa vẫn đang đối diện với nhiều rủi ro về an toàn thông tin. Nhận thức và thực hành về an toàn thông tin tại các doanh nghiệp còn nhiều hạn chế, đặc biệt là hệ thống thông tin kế toán, hệ thống lưu trữ và xử lý các thông tin quan trọng về tài chính, tài sản và dữ liệu kinh doanh. Nhiều doanh nghiệp chưa ban hành đầy đủ chính sách bảo mật, hệ thống kỹ thuật bảo vệ dữ liệu chưa được đầu tư phù hợp, và đội ngũ nhân sự thiếu kỹ năng cũng như nhận thức về an toàn thông tin kế toán, dẫn đến nguy cơ bị tấn công mạng hoặc rò rỉ dữ liệu. Điều này dẫn đến nguy cơ bị tấn công mạng hoặc đánh cắp dữ liệu kế toán, gây tổn thất lớn cho doanh nghiệp. Ngoài ra, việc tỉnh Thanh Hóa đang dần trở thành điểm đến của nhiều doanh nghiệp nước ngoài và sự tham gia sâu rộng của các doanh nghiệp nội địa vào các chuỗi cung ứng quốc tế đòi hỏi phải có một hệ thống bảo mật thông tin mạnh mẽ hơn bao giờ hết. Các yêu cầu quốc tế về bảo mật thông tin và sự minh bạch trong quản lý tài chính càng nhấn mạnh vai trò của VHATTT kế toán trong việc duy trì và phát triển các hoạt động kinh doanh.

Nghiên cứu này nhằm mục đích đánh giá thực trạng VHATTT kế toán tại các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa. Những phát hiện của nghiên cứu này sẽ giúp nhà quản trị có sự hiểu biết sâu sắc hơn về thực trạng VHATTT tại các doanh nghiệp. Trên cơ sở đó, doanh nghiệp có thể xây dựng các chiến lược và chính sách nâng cao VHATTT, góp phần nâng cao tính hữu hiệu của hệ thống thông tin kế toán trong bối cảnh hiện nay.

2. PHƯƠNG PHÁP NGHIÊN CỨU

Phương pháp nghiên cứu được thực hiện thông qua hai bước: Nghiên cứu định tính và nghiên cứu định lượng. Nghiên cứu định tính được tiến hành với mẫu gồm 20 nhà quản trị

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

tại các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa nhằm khám phá nhận thức về các yếu tố của VHATTT tại các đơn vị của họ. Kết quả nghiên cứu định tính giúp tác giả thiết lập công cụ đo lường định lượng.

Nghiên cứu định lượng được tiến hành qua hai giai đoạn. Giai đoạn một, tác giả nghiên cứu thử nghiệm trên nhóm nhỏ nhằm phát hiện những sai sót trong bảng hỏi. Giai đoạn hai, nghiên cứu chính thức và được tiến hành bằng bảng hỏi đã được chỉnh sửa sau giai đoạn thử nghiệm. Cuộc khảo sát được thực hiện vào tháng 12 năm 2024. Đối tượng nghiên cứu được đề nghị trả lời các câu hỏi theo thang đo Likert 5 bậc (từ 1 - hoàn toàn không đồng ý đến 5 - hoàn toàn đồng ý). Bảng hỏi do đáp viên trả lời là công cụ chính để thu thập dữ liệu. Phần mềm xử lý số liệu SPSS 20.0 được dùng cho xử lý và phân tích thống kê.

Thống kê mẫu nghiên cứu: tổng số phiếu điều tra gửi đi là 380 phiếu; số phiếu hợp lệ là 326 được sử dụng cho phân tích. Đối tượng điều tra là các nhà quản lý các cấp (từ cấp phòng trở lên) và nhân viên bộ phận kế toán của các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa, đáp ứng yêu cầu về số lượng và chất lượng cho cuộc khảo sát.

Cụ thể, về giới tính, có 162 nam (49,7%) và 164 nữ (50,3%), cho thấy sự phân bổ khá cân bằng giữa hai nhóm trong mẫu nghiên cứu.

Về độ tuổi, nhóm dưới 30 tuổi chiếm 118 người (36,2%), nhóm từ 31 - 45 tuổi có 142 người (43,6%), và nhóm trên 45 tuổi có 66 người (20,2%). Kết quả này phản ánh lực lượng lao động trong lĩnh vực kế toán và quản lý doanh nghiệp may mặc chủ yếu tập trung vào nhóm tuổi trung niên.

Xét về trình độ học vấn, phần lớn người tham gia khảo sát có trình độ cử nhân (256 người, chiếm 78,5%), trong khi số người có trình độ thạc sĩ là 70 người (21,5%), cho thấy phần lớn nhân sự làm kế toán và quản lý trong các doanh nghiệp này có nền tảng học vấn khá cao.

Về vị trí công việc, có 212 kế toán viên (65,0%) và 114 cán bộ quản lý (35,0%), cho thấy mẫu khảo sát tập trung chủ yếu vào đội ngũ thực hiện trực tiếp công tác kế toán, đồng thời vẫn có sự tham gia đáng kể của các cấp quản lý nhằm cung cấp góc nhìn chiến lược về an toàn thông tin kế toán.

Thang đo: nghiên cứu sử dụng thang đo Likert 5 mức độ, trong đó: 1- Rất không tốt, 2- Không tốt, 3- Bình thường, 4- Tốt, 5- Rất tốt. Kết quả được sử dụng để đánh giá tính hữu hiệu của hệ thống thông tin kế toán theo căn cứ sau đây [11]:

Mức điểm trung bình từ 1,0 đến 1,80: được đánh giá là rất không tốt;

Mức điểm trung bình từ 1,81 đến 2,6: được đánh giá là không tốt;

Mức điểm trung bình từ 2,61 đến 3,40: được đánh giá là bình thường;

Mức điểm trung bình từ 3,41 đến 4,20: được đánh giá là tốt;

Mức điểm trung bình từ 4,21 đến 5,0: được đánh giá là rất tốt.

Kết quả nghiên cứu bao gồm các nội dung chính: khái quát về VHATTT và VHATTT kế toán, đánh giá thực trạng VHATTT kế toán tại các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa, từ đó, đề xuất những kiến nghị góp phần nâng cao VHATTT kế toán tại các đơn vị này.

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

3. KẾT QUẢ NGHIÊN CỨU VÀ THẢO LUẬN

3.1. Khái quát về văn hoá an toàn thông tin

VHATTT đóng vai trò quan trọng trong việc duy trì và cải thiện sự bảo mật của tổ chức, nhằm bảo vệ dữ liệu, hệ thống và thông tin khỏi các mối đe dọa từ cả bên ngoài và bên trong. VHATTT không chỉ phản ánh thái độ và hành vi của các cá nhân trong tổ chức đối với an toàn thông tin, mà còn là sự nhận thức chung về tầm quan trọng của bảo mật và cách thức thực hiện các biện pháp an toàn trong môi trường làm việc. VHATTT có thể được hiểu là một hệ thống các giá trị, niềm tin và hành vi mà các thành viên trong tổ chức tuân thủ để đảm bảo an toàn thông tin. Theo lý thuyết, một nền VHATTT mạnh mẽ bao gồm sự hỗ trợ của các yếu tố như cam kết lãnh đạo, giáo dục và đào tạo người dùng, và các chính sách bảo mật rõ ràng [14]. Các tổ chức phải phát triển và duy trì một văn hóa mà ở đó các thành viên đều nhận thức được trách nhiệm của mình đối với an toàn thông tin. Một nghiên cứu khác nhấn mạnh rằng VHATTT không phải chỉ là về các quy định kỹ thuật, mà còn bao gồm các yếu tố mềm như thái độ, nhận thức và hành vi của người dùng đối với các chính sách và quy trình bảo mật trong tổ chức [8]. Việc xây dựng và duy trì một nền văn hóa này đòi hỏi sự tham gia của tất cả các thành viên trong tổ chức, từ lãnh đạo đến các nhân viên. Như vậy, VHATTT bao gồm một số yếu tố chính như sau:

(1) Nhận thức và thái độ về an toàn thông tin: Nhận thức về các mối đe dọa và tầm quan trọng của an toàn thông tin là yếu tố quan trọng trong việc hình thành văn hóa an toàn. Điều này bao gồm việc nhận thức về các nguy cơ bảo mật, như tấn công mạng, đánh cắp dữ liệu, và sự phát triển của các mối đe dọa công nghệ [6]. Nhận thức về an toàn thông tin được đánh giá dựa trên nhận thức của cán bộ nhân viên về các mối đe dọa an toàn thông tin và tầm quan trọng của các biện pháp bảo mật [9] hoặc đồng tình với các tuyên bố về sự quan trọng của bảo mật thông tin trong công việc tác nghiệp hàng ngày.

(2) Hành vi và thực hành bảo mật: VHATTT không chỉ dựa vào các nhận thức mà còn phải được thể hiện qua hành vi và thói quen bảo mật của người dùng. Hành vi có thể bao gồm việc sử dụng mật khẩu mạnh, việc tuân thủ các chính sách bảo mật, và thái độ đối với việc chia sẻ thông tin [15]. Hành vi và thực hành bảo mật được đánh giá thông qua các hành vi thực tế của người dùng như việc tuân thủ chính sách mật khẩu, việc sử dụng phần mềm bảo mật, và việc tuân thủ các quy trình bảo mật tổ chức. Hay nói cách khác, chính là mức độ chấp hành thực tế của các nhân viên đối với các chính sách an toàn thông tin.

(3) Cam kết của lãnh đạo: Cam kết của các nhà lãnh đạo trong tổ chức là yếu tố quyết định đến việc xây dựng VHATTT. Lãnh đạo cần thể hiện sự quan tâm đến bảo mật thông tin thông qua các chính sách, quyết định tài trợ cho các sáng kiến bảo mật và khuyến khích hành vi bảo mật trong toàn tổ chức. Doanh nghiệp có thể đánh giá mức độ cam kết của lãnh đạo đối với an toàn thông tin, thông qua các sáng kiến và quyết định về chính sách bảo mật, cũng như mức độ tham gia của họ trong các chương trình bảo mật của tổ chức [6].

(4) Đào tạo về an toàn thông tin: Đào tạo liên tục về an toàn thông tin giúp người dùng nhận thức rõ hơn về các rủi ro và cách thức phòng tránh. Các chương trình đào tạo

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

hiệu quả có thể giúp thay đổi hành vi người dùng và giảm thiểu các mối đe dọa bảo mật do yếu tố con người gây ra [17]. Các tổ chức có thể đánh giá hiệu quả của các chương trình đào tạo về an toàn thông tin trong việc thay đổi nhận thức và hành vi của nhân viên, cũng như mức độ tham gia của họ vào các khóa đào tạo bảo mật [19].

VHATTT là một yếu tố quan trọng trong việc bảo vệ dữ liệu của tổ chức khỏi các mối đe dọa. Để xây dựng một văn hóa an toàn hiệu quả, cần phải có sự tham gia của tất cả các thành viên trong tổ chức, từ lãnh đạo đến nhân viên, cũng như sự cam kết mạnh mẽ đối với các chính sách bảo mật. Các thang đo về nhận thức, hành vi, cam kết lãnh đạo và đào tạo là công cụ hữu ích để đánh giá mức độ trưởng thành của VHATTT trong tổ chức.

3.2. Khái quát về văn hóa an toàn thông tin kế toán

VHATTT kế toán bao gồm nhận thức, hành vi, kỹ năng và các quy định liên quan đến bảo vệ thông tin, nhằm bảo đảm rằng tất cả các cá nhân trong doanh nghiệp đều có trách nhiệm và vai trò trong việc bảo mật thông tin [7]. VHATTT kế toán sẽ đảm bảo khi có sự tham gia của tất cả nhà quản trị và nhân viên. Nhân viên cần nhận thức được các mối đe dọa an toàn tiềm ẩn đối với tổ chức, đặc biệt là các sự cố hệ thống thông tin nội bộ [15] và thay đổi hành vi, thái độ, cũng như nhận thức của mọi người để có nhận thức và hiểu biết về hệ thống thông tin kế toán [5].

Mối liên kết giữa VHATTT và tính hữu hiệu của hệ thống thông tin kế toán là một yếu tố không thể thiếu trong việc đảm bảo sự an toàn và hiệu quả của các hệ thống tài chính trong tổ chức. Khi VHATTT được xây dựng và củng cố vững chắc trong tổ chức, nó sẽ có tác động trực tiếp đến khả năng hoạt động hiệu quả và bảo mật của hệ thống thông tin kế toán, từ đó giúp nâng cao chất lượng thông tin tài chính và giảm thiểu các sai sót có thể xảy ra. VHATTT kế toán là tập hợp các giá trị, chuẩn mực, niềm tin và hành vi của tổ chức và cá nhân trong việc bảo vệ, sử dụng và quản lý thông tin kế toán một cách an toàn, hiệu quả [2]. VHATTT kế toán bao gồm cả nhận thức, trách nhiệm và cam kết của các bên liên quan trong việc đảm bảo tính bảo mật, toàn vẹn và sẵn có của thông tin kế toán.

Trong nghiên cứu này, nhóm tác giả xây dựng và sử dụng thang đo đánh giá VHATTT kế toán dựa trên thang đo đánh giá văn hóa hóa an toàn thông tin nói chung, bao gồm 04 thành phần: (1) Nhận thức và thái độ, (2) Hành vi, (3) Cam kết của lãnh đạo, (4) Đào tạo. Các thang đo được điều chỉnh cho phù hợp với thông tin kế toán và tình hình thực tế tại các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa [10][12][6].

3.3. Thực trạng văn hóa an toàn thông tin kế toán tại các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa

3.3.1. Thực trạng nhận thức và thái độ về an toàn thông tin kế toán của các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa

Kết quả khảo sát phản ánh thực trạng nhận thức và thái độ về an toàn thông tin kế toán trong các doanh nghiệp may mặc tại Thanh Hóa, cho thấy mặc dù có sự nhận diện nhất định về các rủi ro bảo mật, nhưng mức độ quan tâm và chủ động thực hiện các biện pháp an toàn vẫn còn hạn chế (bảng 1).

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

Bảng 1. Giá trị trung bình của "Nhận thức và thái độ về an toàn thông tin kế toán"

STT	Thang đo	Giá trị trung bình	Đánh giá
1	Nhận thức được các mối đe dọa bảo mật như tấn công mạng và đánh cắp dữ liệu kế toán là một vấn đề nghiêm trọng.	3,43	Tốt
2	Hiểu rằng an toàn thông tin kế toán là một yếu tố quan trọng đối với công việc của tôi hàng ngày.	3,22	Bình thường
3	Các mối đe dọa công nghệ như virus, phần mềm độc hại là các yếu tố cần phải luôn cảnh giác.	2,78	Bình thường
4	Việc duy trì bảo mật thông tin kế toán giúp bảo vệ quyền lợi cá nhân và tổ chức.	2,81	Bình thường
5	Luôn cố gắng hiểu và cập nhật các biện pháp bảo mật thông tin kế toán trong công việc.	2,43	Không tốt

Nhận thức và thái độ về an toàn thông tin kế toán của các doanh nghiệp may mặc tại Thanh Hóa được đánh giá ở mức trung bình, với điểm trung bình dao động từ 2,43 đến 3,43. Nhân viên có nhận thức khá tốt về mức độ nghiêm trọng của các mối đe dọa bảo mật, với điểm trung bình 3,43, cho thấy họ hiểu rằng tấn công mạng và đánh cắp dữ liệu kế toán là rủi ro đáng lo ngại. Tuy nhiên, mức độ coi trọng an toàn thông tin trong công việc hàng ngày chỉ đạt 3,22 điểm, phản ánh sự quan tâm chưa cao. Chẳng hạn, tại Công ty TNHH May Tiên Sơn, Thanh Hóa - một doanh nghiệp may mặc quy mô lớn với hơn 3.000 lao động, khảo sát cho thấy, phần lớn nhân viên kế toán nhận thức được nguy cơ mất an toàn thông tin nhưng vẫn chủ quan trong việc thực hiện các biện pháp bảo mật. Hệ thống kế toán của công ty từng bị tấn công bởi phần mềm độc hại do nhân viên vô tình mở email lạ, gây mất dữ liệu quan trọng. Tuy vậy, việc đào tạo nhân viên về an toàn thông tin vẫn chưa được coi là ưu tiên hàng đầu. Tương tự, tại Công ty cổ phần May xuất khẩu Trường Thắng, mặc dù lãnh đạo doanh nghiệp đã ban hành các quy định về bảo mật dữ liệu, nhưng nhiều nhân viên vẫn chưa có ý thức duy trì bảo mật thông tin kế toán để bảo vệ quyền lợi cá nhân và tổ chức, với điểm đánh giá chỉ đạt 2,81. Đáng chú ý, mức độ chủ động trong việc cập nhật và tìm hiểu biện pháp bảo mật tại công ty này rất thấp (2,43 điểm). Chỉ một số ít nhân viên chủ động cập nhật kiến thức bảo mật, trong khi phần lớn vẫn chưa quan tâm đến việc thay đổi mật khẩu định kỳ hoặc sử dụng phần mềm bảo mật chuyên dụng. Để cải thiện tình trạng này, các doanh nghiệp cần tăng cường đào tạo, xây dựng văn hóa bảo mật và áp dụng các quy trình kiểm soát chặt chẽ hơn nhằm giảm thiểu rủi ro mất an toàn thông tin trong kế toán.

3.3.2. Thực trạng hành vi an toàn thông tin kế toán của các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa

Kết quả khảo sát phản ánh sự chênh lệch trong hành vi an toàn thông tin kế toán của các doanh nghiệp may mặc tại Thanh Hóa, khi nhân viên có ý thức tuân thủ chính sách bảo mật nhưng chưa chủ động trong việc sử dụng các công cụ bảo vệ dữ liệu (bảng 2).

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

Bảng 2. Giá trị trung bình của "Hành vi an toàn thông tin kế toán"

STT	Thang đo	Giá trị trung bình	Đánh giá
1	Luôn sử dụng mật khẩu mạnh và thay đổi mật khẩu định kỳ.	3,11	Bình thường
2	Tuân thủ đầy đủ các chính sách bảo mật do công ty quy định, bao gồm việc không chia sẻ mật khẩu hay thông tin cá nhân.	4,21	Rất tốt
3	Sử dụng phần mềm bảo mật được tổ chức cung cấp để bảo vệ dữ liệu cá nhân và công ty.	2,42	Không tốt
4	Thực hiện kiểm tra bảo mật và cập nhật phần mềm thường xuyên để bảo vệ thiết bị cá nhân và máy tính làm việc.	3,79	Tốt
5	Hiểu rằng việc chia sẻ thông tin nhạy cảm một cách không an toàn có thể gây hại cho tổ chức.	4,29	Rất tốt

(Nguồn: Xử lý dữ liệu của tác giả)

Kết quả khảo sát cho thấy hành vi an toàn thông tin kế toán của các doanh nghiệp may mặc tại Thanh Hóa có sự chênh lệch đáng kể giữa các khía cạnh, với điểm trung bình dao động từ 2,42 đến 4,29. Nhân viên có ý thức tuân thủ tốt các chính sách bảo mật của công ty, thể hiện qua điểm số 4,21, và nhận thức rõ ràng về rủi ro từ việc chia sẻ thông tin nhạy cảm không an toàn, với mức đánh giá 4,29 điểm - đây là hai yếu tố có mức độ thực hiện cao nhất. Tại Công ty TNHH May xuất khẩu An Hoàng Sơn, một doanh nghiệp may mặc lớn với hệ thống kế toán được quản lý bằng phần mềm ERP, phần lớn nhân viên kế toán tuân thủ nghiêm túc chính sách bảo mật, không chia sẻ mật khẩu hoặc thông tin quan trọng ra bên ngoài. Điều này giúp doanh nghiệp đạt mức điểm cao (4,29) về nhận thức rủi ro khi chia sẻ thông tin. Tuy nhiên, việc sử dụng phần mềm bảo mật vẫn chưa được coi trọng, với nhiều nhân viên chỉ dựa vào hệ thống có sẵn thay vì chủ động cài đặt các công cụ bảo vệ dữ liệu cá nhân, dẫn đến điểm số 2,42 thấp nhất trong khảo sát. Tại Công ty cổ phần May Minh Anh Thọ Xuân, mặc dù doanh nghiệp đã yêu cầu nhân viên thay đổi mật khẩu định kỳ, nhưng khảo sát cho thấy nhiều nhân viên vẫn sử dụng mật khẩu yếu hoặc đặt lại mật khẩu giống nhau, khiến mức điểm chỉ đạt 3,11. Việc kiểm tra bảo mật và cập nhật phần mềm thường xuyên tại công ty này được đánh giá khá tốt (3,79), do bộ phận IT có trách nhiệm nhắc nhở nhân viên cập nhật phần mềm kế toán và diệt virus định kỳ. Tuy nhiên, công ty chưa áp dụng xác thực hai yếu tố trên toàn bộ hệ thống kế toán, khiến dữ liệu vẫn tiềm ẩn nguy cơ bị truy cập trái phép. Một số doanh nghiệp đã bắt đầu triển khai các biện pháp bảo mật mạnh mẽ hơn như xác thực hai yếu tố, mã hóa dữ liệu, nhưng nhìn chung, nhiều doanh nghiệp vẫn chưa có quy trình kiểm tra bảo mật định kỳ. Để cải thiện tình trạng này, các doanh nghiệp cần nâng cao ý thức cho nhân viên về việc sử dụng phần mềm bảo mật, thay đổi mật khẩu định kỳ và chủ động thực hiện các biện pháp bảo vệ dữ liệu nhằm giảm thiểu rủi ro mất an toàn thông tin kế toán

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

3.3.3. Thực trạng cam kết của lãnh đạo về an toàn thông tin kế toán của các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa

Cam kết của lãnh đạo về an toàn thông tin kế toán trong các doanh nghiệp may mặc tại Thanh Hóa còn hạn chế, mặc dù nhiều doanh nghiệp đã ban hành chính sách bảo mật, nhưng việc lồng ghép bảo mật vào chiến lược phát triển còn hạn chế, và nguồn lực dành cho các biện pháp kỹ thuật như mã hóa, giám sát truy cập hoặc đào tạo vẫn chưa được quan tâm đúng mức (bảng 3).

Bảng 3. Giá trị trung bình của "Cam kết của lãnh đạo"

STT	Thang đo	Giá trị trung bình	Đánh giá
1	Lãnh đạo của tổ chức thể hiện rõ sự quan tâm đến bảo mật thông tin kế toán thông qua các chính sách bảo mật.	3,49	Tốt
2	Lãnh đạo của tổ chức khuyến khích hành vi bảo mật trong toàn tổ chức và nhấn mạnh tầm quan trọng của việc bảo vệ thông tin kế toán	2,89	Bình thường
3	Các quyết định về bảo mật thông tin kế toán được ưu tiên trong các chiến lược và kế hoạch của tổ chức.	2,43	Không tốt
4	Các nhà lãnh đạo tham gia trực tiếp vào các chương trình bảo mật thông tin kế toán của tổ chức.	2,92	Bình thường
5	Lãnh đạo tổ chức cam kết tài trợ cho các sáng kiến bảo mật để đảm bảo an toàn thông tin kế toán	1,81	Rất không tốt

Với điểm trung bình dao động từ 1,81 đến 3,49, là thể hiện sự quan tâm nhất định của lãnh đạo đến bảo mật thông tin kế toán thông qua các chính sách bảo mật (với mức điểm 3,49 cho thấy cam kết ở mức tốt). Tại Công ty cổ phần May xuất khẩu Trường Thắng, ban lãnh đạo đã ban hành các chính sách bảo mật thông tin kế toán, yêu cầu nhân viên tuân thủ nghiêm ngặt các quy trình bảo mật khi xử lý dữ liệu tài chính. Tuy nhiên, việc khuyến khích nhân viên thực hiện các hành vi bảo mật vẫn chưa được chú trọng, với điểm đánh giá chỉ đạt 2,89. Nhiều nhân viên kế toán của công ty cho biết họ không thường xuyên nhận được sự nhấn mạnh từ cấp quản lý về tầm quan trọng của bảo mật thông tin. Trong khi đó, tại Công ty cổ phần May xuất khẩu Trường Thắng, dù lãnh đạo có nhận thức về an toàn thông tin kế toán nhưng chưa ưu tiên việc tích hợp bảo mật vào chiến lược phát triển lâu dài. Điểm số 2,43 phản ánh thực trạng bảo mật chưa được xem là yếu tố cốt lõi trong kế hoạch kinh doanh của doanh nghiệp. Sự tham gia trực tiếp của lãnh đạo vào các chương trình bảo mật tại công ty này cũng chỉ đạt 2,92 điểm, cho thấy họ chưa chủ động giám sát hoặc thúc đẩy các hoạt động nâng cao nhận thức về bảo mật trong nội bộ. Đặc biệt, mức độ cam kết tài trợ cho các sáng kiến bảo mật tại công ty này chỉ đạt 1,81 điểm - thấp nhất trong số các chỉ tiêu khảo sát. Điều này phản ánh việc doanh nghiệp chưa sẵn sàng đầu tư tài chính vào các giải pháp bảo mật như hệ thống tường lửa nâng cao, phần mềm mã hóa dữ liệu hay đào tạo chuyên sâu cho nhân viên. Một số doanh nghiệp đã có chính sách bảo mật nhưng thiếu ngân sách để triển khai đồng bộ các giải pháp công nghệ và đào tạo nguồn nhân lực. Để cải thiện thực trạng này, lãnh đạo doanh nghiệp cần nâng cao nhận thức về tầm quan trọng của an toàn thông tin kế toán, đồng thời có chiến lược đầu tư dài hạn vào hạ tầng bảo mật và đào tạo nhân sự nhằm giảm thiểu rủi ro mất an toàn thông tin trong hoạt động kế toán.

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

3.3.4. Thực trạng đào tạo về an toàn thông tin kế toán của các doanh nghiệp may mặc trên địa bàn tỉnh Thanh Hóa

Hoạt động đào tạo về an toàn thông tin kế toán trong các doanh nghiệp may mặc tại Thanh Hóa còn hạn chế, khi số lượng khóa đào tạo ít, chất lượng chưa cao, và chưa thực sự giúp nhân viên thay đổi hành vi bảo mật một cách rõ rệt (bảng 4).

Bảng 4. Giá trị trung bình của "Đào tạo"

STT	Thang đo	Giá trị trung bình	Đánh giá
1	Đã tham gia ít nhất một khóa đào tạo về an toàn thông tin trong năm qua.	1,79	Rất không tốt
2	Các chương trình đào tạo về an toàn thông tin kế toán trong tổ chức giúp cán bộ nhân viên hiểu rõ hơn về các rủi ro bảo mật và cách phòng tránh.	2,17	Không tốt
3	Sau khi tham gia đào tạo, cán bộ nhận viên nhận thức được tầm quan trọng của việc bảo mật thông tin kế toán hơn	2,73	Bình thường
4	Các khóa đào tạo về an toàn thông tin kế toán đã giúp cán bộ nhân viên thay đổi hành vi và thói quen bảo mật của mình.	3,11	Bình thường
5	Các chương trình đào tạo cung cấp cho cán bộ nhân viên những công cụ và kỹ năng cần thiết để bảo vệ thông tin kế toán.	3,27	Bình thường

Kết quả khảo sát đã phản ánh nhiều tồn tại trong công tác đào tạo về an toàn thông tin kế toán tại các doanh nghiệp may mặc ở Thanh Hóa, với điểm trung bình dao động từ 1,79 đến 3,27. Đáng chú ý, tỷ lệ nhân viên tham gia ít nhất một khóa đào tạo về an toàn thông tin trong năm qua rất thấp, với điểm 1,79, cho thấy hoạt động đào tạo chưa được triển khai thường xuyên. Tại Công ty CP May xuất khẩu Trường Thắng, trong năm qua, chỉ có một số ít nhân viên kế toán tham gia các khóa đào tạo về an toàn thông tin, chủ yếu là các buổi phổ biến quy định nội bộ thay vì các chương trình huấn luyện chuyên sâu. Điều này phản ánh thực trạng đào tạo chưa thực sự hiệu quả, khi điểm số đánh giá về mức độ giúp nhân viên hiểu rõ rủi ro bảo mật chỉ đạt 2,17. Nhân viên sau khi tham gia đào tạo có nhận thức tốt hơn về tầm quan trọng của bảo mật thông tin kế toán (2,73 điểm), nhưng hành vi bảo mật chưa thay đổi đáng kể (3,11 điểm).

Tại Công ty cổ phần May Thanh Hóa, dù đã tổ chức các khoá đào tạo về an toàn thông tin kế toán nhưng chương trình chủ yếu mang tính lý thuyết, chưa cung cấp đầy đủ công cụ thực hành. Nhân viên kế toán được hướng dẫn các nguyên tắc bảo mật cơ bản nhưng chưa có nhiều kỹ năng xử lý tình huống thực tế khi xảy ra sự cố an ninh mạng. Điểm số đánh giá về mức độ chương trình đào tạo cung cấp công cụ và kỹ năng cần thiết chỉ đạt 3,27, cho thấy vẫn chưa đáp ứng kỳ vọng.

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

Ngoài ra, một số doanh nghiệp chỉ tổ chức đào tạo dưới hình thức phổ biến văn bản thay vì thực hành thực tế, dẫn đến nhân viên không có kỹ năng xử lý các tình huống bảo mật khi xảy ra sự cố. Để cải thiện tình trạng này, các doanh nghiệp cần xây dựng chương trình đào tạo bài bản, kết hợp thực hành với các tình huống giả lập thực tế nhằm nâng cao khả năng ứng phó của nhân viên trước các nguy cơ mất an toàn thông tin kế toán.

3.4. Thảo luận và kiến nghị

Kết quả phân tích cho thấy VHATTT kế toán tại các doanh nghiệp may mặc ở Thanh Hóa còn nhiều hạn chế:

Thứ nhất, nhận thức và thái độ về an toàn thông tin kế toán của nhân viên đạt mức trung bình, với sự hiểu biết nhất định về rủi ro bảo mật nhưng chưa chủ động trong việc cập nhật kiến thức và áp dụng các biện pháp bảo mật. Nhân viên nhận thức được tầm quan trọng của việc bảo vệ thông tin kế toán, nhưng mức độ thực hiện các biện pháp an toàn vẫn còn thấp, đặc biệt là trong việc cập nhật thông tin bảo mật thường xuyên.

Thứ hai, cán bộ quản lý và nhân viên tuân thủ tốt các quy định bảo mật do doanh nghiệp đề ra nhưng lại chưa chủ động sử dụng phần mềm bảo mật hoặc thay đổi mật khẩu định kỳ. Điều này cho thấy mặc dù có sự tuân thủ quy định, nhưng ý thức tự giác trong bảo vệ thông tin vẫn chưa cao, dẫn đến nguy cơ rò rỉ dữ liệu.

Thứ ba, cam kết của lãnh đạo đối với an toàn thông tin kế toán chưa thực sự rõ ràng. Mặc dù lãnh đạo doanh nghiệp thể hiện sự quan tâm thông qua chính sách bảo mật, nhưng mức độ ưu tiên bảo mật trong chiến lược phát triển còn thấp. Đặc biệt, cam kết tài trợ cho các sáng kiến bảo mật rất hạn chế, làm giảm hiệu quả triển khai các biện pháp bảo mật trong tổ chức.

Thứ tư, công tác đào tạo về an toàn thông tin kế toán chưa được chú trọng. Phần lớn nhân viên chưa từng tham gia các khóa đào tạo chuyên sâu, khiến họ thiếu kỹ năng nhận diện và xử lý rủi ro bảo mật. Các chương trình đào tạo chưa đủ thực tế và chưa tạo ra sự thay đổi đáng kể trong nhận thức và hành vi bảo mật của nhân viên.

Để xây dựng, duy trì và tăng cường VHATTT kế toán, nhóm tác giả đề xuất một số kiến nghị đối với các doanh nghiệp may mặc tại Thanh Hóa như sau:

Thứ nhất, tăng cường tuyên truyền và nâng cao nhận thức về bảo mật thông tin: Doanh nghiệp cần tổ chức các chương trình tuyên truyền thường xuyên nhằm giúp nhân viên nhận thức rõ về tầm quan trọng của an toàn thông tin kế toán; khuyến khích nhân viên cập nhật kiến thức về bảo mật, thực hành các biện pháp an toàn thông tin trong công việc hàng ngày, đặc biệt là trong xử lý dữ liệu kế toán và tài chính.

Thứ hai, tăng cường chính sách bảo mật thông tin cá nhân và dữ liệu kế toán: Doanh nghiệp cần xây dựng và phổ biến các chính sách bảo mật rõ ràng, bao gồm quy định về sử dụng mật khẩu mạnh và yêu cầu thay đổi định kỳ. Đồng thời, doanh nghiệp cần trang bị phần mềm bảo mật phù hợp và khuyến khích nhân viên sử dụng đúng cách nhằm giảm thiểu nguy cơ rò rỉ dữ liệu.

Thứ ba, đưa an toàn thông tin kế toán vào chiến lược phát triển doanh nghiệp: Lãnh đạo doanh nghiệp cần coi an toàn thông tin kế toán là một phần quan trọng trong chiến

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

lược phát triển, không chỉ là vấn đề kỹ thuật mà còn là yếu tố quyết định đến sự bền vững của doanh nghiệp; đồng thời, cần ưu tiên đầu tư tài chính cho các giải pháp bảo mật tiên tiến, như hệ thống tường lửa, phần mềm chống virus, hệ thống quản lý truy cập để bảo vệ dữ liệu kế toán khỏi các rủi ro an ninh mạng. Ngoài ra, ban lãnh đạo cần tham gia tích cực vào các chương trình nâng cao nhận thức an toàn thông tin, làm gương trong việc tuân thủ các quy định bảo mật.

Thứ tư, tổ chức các khóa đào tạo định kỳ về an toàn thông tin: Các doanh nghiệp cần xây dựng chương trình đào tạo an toàn thông tin dành riêng cho từng nhóm nhân viên, từ nhân viên kế toán, nhân sự đến quản lý cấp cao. Các khóa đào tạo nên kết hợp giữa lý thuyết và thực hành, giúp nhân viên nhận diện và xử lý hiệu quả các rủi ro bảo mật như tấn công lừa đảo, mã độc xâm nhập trái phép. Việc đào tạo nên được cá nhân hóa theo từng cấp độ nhân viên, đảm bảo nội dung phù hợp với đặc thù công việc và mức độ tiếp cận thông tin quan trọng của từng vị trí.Việc thực hiện đồng bộ các kiến nghị trên sẽ giúp nâng cao nhận thức, hành vi và cam kết của cả nhân viên lẫn lãnh đạo, từ đó góp phần xây dựng một VHATTT kế toán bền vững cho các doanh nghiệp may mặc tại Thanh Hóa.

4. KẾT LUẬN

Kết quả nghiên cứu cho thấy VHATTT kế toán tại các doanh nghiệp may mặc ở Thanh Hóa còn nhiều hạn chế, đặc biệt ở các khía cạnh nhận thức, hành vi, cam kết của lãnh đạo và công tác đào tạo. Nhân viên tuy có ý thức về an toàn thông tin nhưng chưa chủ động áp dụng biện pháp bảo mật, trong khi lãnh đạo chưa ưu tiên đầu tư cho bảo mật. Việc tuân thủ quy định bảo mật còn mang tính hình thức, thiếu sự chủ động trong thực tế. Công tác đào tạo về an toàn thông tin chưa được chú trọng, dẫn đến hạn chế trong nhận diện và xử lý rủi ro. Để nâng cao VHATTT các doanh nghiệp cần tăng cường đào tạo, nâng cao ý thức bảo mật, đầu tư công nghệ và tích cực thực hiện các biện pháp bảo vệ dữ liệu kế toán.

TÀI LIỆU THAM KHẢO

[1] Cục thống kê tỉnh Thanh Hóa (2025), *Báo cáo Tình hình kinh tế - xã hội tháng 01 năm 2025*.

[2] Nguyễn Ngọc Khánh Dung (2023), *Ảnh hưởng của văn hóa tổ chức đến chất lượng hệ thống thông tin kế toán trong các doanh nghiệp nhỏ và vừa ở Việt Nam*, Tạp chí Khoa học và Công nghệ, 66(06):45-57.

[3] Thủ tướng Chính phủ (2023), *Quyết định số 153/QĐ-TTg phê duyệt Quy hoạch tỉnh Thanh Hóa thời kỳ 2021 - 2030, tầm nhìn đến năm 2045*.

[4] Trần Thị Hằng, Đào Thu Hà (2022), *Công nghệ Blockchain trong ngành kế toán - kiểm toán,* Kỷ yếu Hội thảo khoa học quốc gia về Kế toán và Kiểm toán.

[5] Vũ Hồng Sơn (2023), *Ứng dụng mô hình quản trị rủi ro trong đảm bảo an toàn thông tin kế toán tại Việt Nam,* Tạp chí Tài chính, 2023(3):12-19.

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

[6] Vũ Quốc Thông (2023), *Nhân tố ảnh hưởng đến chất lượng hệ thống thông tin kế toán các doanh nghiệp tại An Giang*, Tạp chí Tài chính kỳ 2 tháng 7, https://tapchitaichinh.vn/nhan-to-anh-huong-den-chat-luong-he-thong-thong-tin-ke-toan-cac-doanh-nghiep-tai-an-giang.html

[7] AlHogail, A., Mirza, A. (2014), *Information security culture: A definition and a literature review*, In 2014 World Congress on Computer Applications and Information Systems (WCCAIS), IEEE.

[8] Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., Ismail, A. (2022), *Determinants of information security awareness and behaviour strategies in public sector organizations among employees,* International Journal of Advanced Computer Science and Applications, 13(8):479-490.

[9] Anderson, R., Boehme, R., Wright, P. (2012), *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley.

[10] Ayanbode, N., Abieba, O. A., Chukwurah, N., Ajayi, O. O., Ifesinachi, A. (2024), *Human factors in fintech cybersecurity: addressing insider threats and behavioral risks*. Journal of Cybersecurity in FinTech, 14(2):34-49.

[11] Gorla, N., Somers, T. M., Wong, B. (2010), *Organizational impact of system quality, information quality, and service quality*, The Journal of Strategic Information Systems, 19(3):207-228.

[12] Hanifi, F., Taleei, A. (2015), *Accounting information system and management's decision making process*. Management Science Letters, 5(7):685-694.

[13] Hovav, A., D'Arcy, J. (2012), *Security Policy Compliance: A Study of the Role of Employees in Organizational Security*. Computers & Security, 31(4):491-502.

[14] Kabeireho, M. (2020), *Impact of deterrence and user awareness on insider threat vulnerability: A correlational study*, Doctoral dissertation, Capella University.

[15] Li, W., Bhutto, T. A., Nasiri, A. R., Shaikh, H. A., Samo, F. A. (2018), *Organizational innovation: the role of leadership and organizational culture*. International Journal of Public Leadership, 14(1):33-47.

[16] Line, M. B. (2015), *Understanding information security incident management practices: a case study in the electric power industry*, Doctoral dissertation, Norwegian University of Science and Technology.

[17] Niekerk, J. F., Von Solms, R. (2010). *Information security culture: A management perspective*, Computers & security, 29(4):476-486.

[18] Nurwanah, A. (2024), *Cybersecurity in accounting information systems: Challenges and solutions*, Advances in Applied Accounting Research, 2(3):157-168.

[19] Safa, N. S., Von Solms, R., Furnell, S. (2016), *Information security policy compliance model in organizations*, Computers & security, 56:70-82.

p-ISSN 3030 - 4679
e-ISSN 3030 - 4687

THE CURRENT STATE OF ACCOUNTING INFORMATION SECURITY CULTURE IN GARMENT ENTERPRISES IN THANH HOA PROVINCE

Dang Lan Anh, Le Thi Oanh, Hoang Thi Ngoc, Pham Hung Anh

ABSTRACT

This study emphasizes the crucial role and assesses the current state of information security culture (ISC) in safeguarding accounting information within garment enterprises in Thanh Hóa province. In the digitalization era, businesses face numerous cybersecurity risks, yet awareness and security practices remain limited. The research employs both qualitative and quantitative methods, with a survey sample of 326 managers and accounting staff from 287 garment enterprises in Thanh Hóa. The findings highlight the strengths and limitations of information security culture through four key factors: awareness, behavior, leadership commitment, and training. Based on these insights, the study proposes recommendations to build, maintain, and enhance the information security culture in accounting within these enterprises.

Keywords: *Information security culture, garment enterprises, Thanh Hóa.*

** Ngày nộp bài: 4/3/2025; Ngày gửi phản biện: 18/3/2025; Ngày duyệt đăng: 30/7/2025*