



# CỤC THÔNG TIN VÀ KHOA HỌC CÔNG NGHỆ QUỐC GIA

Địa chỉ: 24, Lý Thường Kiệt, Hoàn Kiếm, Hà Nội.

Tel: (024) 38262718, Fax: (024) 39349127

## BAN BIÊN TẬP

**TS. Trần Đức Hiến** (Trưởng ban); **ThS. Trần Thị Thu Hà** (Phó Trưởng ban)  
**KS. Nguyễn Mạnh Quân**; **ThS. Nguyễn Lê Hằng**; **ThS. Phùng Anh Tiến**

---

## MỤC LỤC

<b>LỜI NÓI ĐẦU</b> .....	<b>1</b>
<b>DANH MỤC CHỮ VIẾT TẮT</b> .....	<b>2</b>
<b>TÓM TẮT</b> .....	<b>3</b>
<b>I. KHẢ NĂNG TIẾP CẬN CÔNG NGHỆ SỐ VÀ HỖ TRỢ DOANH NGHIỆP VỪA VÀ NHỎ CHUYỂN ĐỔI SỐ</b> .....	<b>5</b>
1.1. Lợi ích của chuyển đổi số .....	5
1.2. Xu hướng phổ biến công nghệ số .....	7
1.3. Tác động của đại dịch COVID-19 đến chuyển đổi số .....	12
1.4. Chính sách hỗ trợ chuyển đổi số cho doanh nghiệp vừa và nhỏ.....	18
<b>II. TĂNG CƯỜNG BẢO MẬT KỸ THUẬT SỐ CHO DOANH NGHIỆP VỪA VÀ NHỎ</b> .....	<b>36</b>
2.1. Thách thức trong việc tăng cường bảo mật kỹ thuật số .....	36
2.2. Quản lý rủi ro kỹ thuật số .....	43
<b>KẾT LUẬN</b> .....	<b>56</b>
<b>TÀI LIỆU THAM KHẢO CHÍNH</b> .....	<b>58</b>

## LỜI NÓI ĐẦU

Trong những năm gần đây, quá trình chuyển đổi số doanh nghiệp vừa và nhỏ (DNVVN) tiếp tục diễn ra mạnh mẽ. Chuyển đổi số mở ra nhiều cơ hội cho DNVVN cải thiện hiệu suất, thúc đẩy đổi mới sáng tạo, nâng cao năng suất và cạnh tranh bình đẳng hơn với các doanh nghiệp lớn.

Tuy nhiên, quy mô nhỏ là rào cản khiến DNVVN bị tụt hậu trong quá trình chuyển đổi số, đặc biệt là do thiếu nguồn lực nội bộ và nhận thức, thiếu hụt kỹ năng hoặc tài chính. Hơn nữa, khả năng tiếp cận và ứng dụng các công nghệ số của DNVVN còn hạn chế. Để dỡ bỏ những rào cản đó và cho phép DNVVN khai thác đầy đủ những lợi ích của quá trình chuyển đổi số, thì chỉ riêng DNVVN không thể làm được mà cần có sự hỗ trợ của các nhà hoạch định chính sách, là nền tảng xây dựng các chính sách kỹ thuật số cho DNVVN trong hiện tại và tương lai.

Cuộc khủng hoảng COVID-19 đã nâng cao tầm quan trọng của chuyển đổi số trong DNVVN. Tuy nhiên, đây cũng là cơ hội cho tin tặc tăng cường tấn công nhằm vào điểm yếu của DNVVN, đó là thiếu sự chuẩn bị để ứng phó với các mối đe dọa ngày càng tinh vi. Vì thế, một số DNVVN đã phải chịu tổn thất lớn. Nhằm giúp DNVVN thích ứng với văn hóa và quy trình hoạt động trong thế giới kỹ thuật số, một số quốc gia đã tìm cách lồng ghép các cân nhắc chính sách DNVVN trong các chương trình chính sách, trong khi các quốc gia khác lại nhằm vào DNVVN với các công cụ thường được điều chỉnh cho phù hợp với từng nơi hoặc ngành cụ thể.

Tổng luận “*Những cân nhắc chính sách hỗ trợ doanh nghiệp vừa và nhỏ chuyển đổi số và tăng cường bảo mật kỹ thuật số*” đề cập đến quá trình chuyển đổi số của DNVVN tại các quốc gia OECD và tập trung phân tích các xu hướng gần đây trong việc tiếp cận và ứng dụng các công nghệ số của DNVVN, cả trong bối cảnh khủng hoảng COVID-19. Đồng thời, tổng luận cũng giới thiệu các chính sách của chính phủ các nước hỗ trợ DNVVN chuyển đổi số và tăng cường quản lý rủi ro kỹ thuật số.

Xin trân trọng giới thiệu!

CỤC THÔNG TIN KHOA HỌC VÀ  
CÔNG NGHỆ QUỐC GIA

## DANH MỤC CHỮ VIẾT TẮT

CNTT&TT	Công nghệ Thông tin và Truyền thông
CRM	Phần mềm Quản lý quan hệ khách hàng
ERP	Lập kế hoạch nguồn lực doanh nghiệp
DNVVN	Doanh nghiệp vừa và nhỏ
ĐTĐM	Điện toán đám mây
EU	Liên minh châu Âu
IoT	Internet kết nối vạn vật
OECD	Tổ chức Hợp tác và Phát triển Kinh tế
SCM	Phần mềm Quản lý chuỗi cung ứng
SHTT	Sở hữu trí tuệ

## TÓM TẮT

Chuyển đổi số đang diễn ra mạnh mẽ cùng với sự phát triển nhanh chóng của công nghệ, đã tạo ra những thay đổi lớn cho các doanh nghiệp thuộc mọi loại hình và lĩnh vực khác nhau. Trong bối cảnh hiện nay, chuyển đổi số cần cho sự phát triển của doanh nghiệp. Ngày càng có nhiều doanh nghiệp tham gia chuyển đổi số và đạt được những thành tựu đáng kể.

Theo Verhoef et al. (2021), chuyển đổi số trong doanh nghiệp đòi hỏi phải có nguồn lực, cơ cấu, chiến lược tăng trưởng, các chỉ số và mục tiêu tương ứng với từng giai đoạn cụ thể. Chuyển đổi số là sự kết hợp của các nguồn lực bổ sung vì nó là một quá trình kỹ thuật xã hội. OECD (2017) khẳng định, để ứng dụng thành công công nghệ thông tin và truyền thông (CNTT&TT) trong DNVVN, thì cần sử dụng tối ưu các tài sản bổ sung dựa vào tri thức như tổ chức và nguồn nhân lực. Các tài sản này cho phép DNVVN giảm lệ thuộc quá mức vào một công nghệ hoặc nền tảng nào đó. Việc không chú trọng đầu tư cho yếu tố con người có thể làm chậm quá trình ứng dụng và phổ biến công nghệ tại các DNVVN.

Chuyển đổi số mở ra nhiều cơ hội cho DNVVN cải thiện hiệu suất, thúc đẩy đổi mới sáng tạo, nâng cao năng suất và cạnh tranh bình đẳng hơn với các doanh nghiệp lớn. Mặc dù trong những năm gần đây, DNVVN vẫn đang nỗ lực chuyển đổi số, nhưng không phải tất cả DNVVN đều có đủ năng lực chuyển đổi. Các doanh nghiệp càng nhỏ, thì càng ít khả năng áp dụng các phương thức kỹ thuật số mới và càng hạn chế việc tiếp nhận các dịch vụ cơ bản. Nhìn chung, chuyển đổi số trong DNVVN có liên quan chặt chẽ đến cách thức tạo ra giá trị trong doanh nghiệp và lĩnh vực hoạt động của doanh nghiệp.

DNVVN có xu hướng số hóa đầu tiên là các chức năng quản trị chung hoặc tiếp thị. Các cuộc khảo sát doanh nghiệp về ứng dụng CNTT&TT cho thấy khoảng cách kỹ thuật số giữa DNVVN và các doanh nghiệp lớn là nhỏ trong các tương tác trực tuyến với chính phủ, trong việc lập hóa đơn điện tử hoặc sử dụng mạng xã hội hoặc bán hàng trực tuyến. Tuy nhiên, khoảng cách giữa các DNVVN về việc áp dụng công nghệ mở rộng khi các công nghệ trở nên tinh vi hơn (như phân tích dữ liệu) hoặc nhiều vấn đề triển khai thực hiện (như lập kế hoạch nguồn lực doanh nghiệp để tích hợp quy trình). Ngoài ra, còn có sự khác biệt rõ nét giữa các doanh nghiệp trong việc sử dụng điện toán đám mây (ĐTĐM).

Khi số hóa các chức năng kinh doanh, DNVVN có xu hướng thuê chuyên gia bên ngoài thực hiện vì năng lực nội bộ còn hạn chế nhưng cũng dựa trên cơ sở chi phí. Ví dụ, các nền tảng số (như mạng xã hội, thị trường thương mại điện tử...)

phục vụ cho việc tối ưu hóa các chức năng nhất định có chi phí rất thấp (như dịch vụ phân tích dữ liệu). Tương tự, để quản lý rủi ro bảo mật kỹ thuật số, DNVVN có xu hướng dựa vào các chuyên gia tư vấn bên ngoài hoặc các tính năng bảo mật theo thiết kế của các sản phẩm và dịch vụ mà họ sử dụng.

Cuộc khủng hoảng COVID-19 đã nâng cao tầm quan trọng của chuyển đổi số trong DNVVN. Các doanh nghiệp đã chuyển sang hoạt động trực tuyến và triển khai các giải pháp làm việc thông minh để duy trì hoạt động kinh doanh trong thời gian phong tỏa và khắc phục sự gián đoạn trong chuỗi cung ứng, với các nền tảng trực tuyến đóng vai trò quan trọng kết nối người dùng với các thị trường, nhà cung cấp hoặc nguồn lực mới. Theo kết quả khảo sát doanh nghiệp trên toàn thế giới, 70% DNVVN đã tăng cường sử dụng công nghệ số do tác động của COVID-19.

Tuy nhiên, bối cảnh COVID-19 cũng tạo cơ hội cho tin tặc tăng cường tấn công nhằm vào điểm yếu của DNVVN, đó là thiếu sự chuẩn bị để ứng phó với các mối đe dọa ngày càng tinh vi. Thật vậy, DNVVN có mức đầu tư thấp cho bảo mật kỹ thuật số và thường là hiểu biết hạn chế về hậu quả của những mối đe dọa đó. Trên thực tế, DNVVN có ít điểm cho tin tặc tấn công, do cường độ kỹ thuật số thấp hơn (mức độ tiếp xúc) và khối lượng (và giá trị) dữ liệu hoặc tài sản trí tuệ nhỏ hơn. Tuy nhiên, khi DNVVN bị ảnh hưởng, tổn thất có khi bằng doanh thu nhiều tháng, vượt xa mức dự trữ trung bình sẵn có của doanh nghiệp.

Các nhà hoạch định chính sách đóng vai trò quan trọng trong việc giúp DNVVN thích ứng văn hóa và quy trình hoạt động trong thế giới kỹ thuật số. Một số quốc gia đã tìm cách lồng ghép các cân nhắc chính sách DNVVN trong các chương trình chính sách khác, trong khi một số khác lại nhằm vào DNVVN với các công cụ thường được điều chỉnh cho phù hợp với các địa điểm hoặc ngành cụ thể.

Các can thiệp chính sách bao gồm: chiến dịch nâng cao nhận thức; đào tạo và hỗ trợ công nghệ; tiếp cận tài chính; hỗ trợ phát triển các giải pháp kỹ thuật số phù hợp với DNVVN; trung tâm dữ liệu, nền tảng thử nghiệm và chương trình mạng; cải cách quy định (như bảo vệ dữ liệu); chính phủ điện tử và một cửa liên thông; và đầu tư cơ sở hạ tầng.

# **I. KHẢ NĂNG TIẾP CẬN CÔNG NGHỆ SỐ VÀ HỖ TRỢ DOANH NGHIỆP VỪA VÀ NHỎ CHUYỂN ĐỔI SỐ**

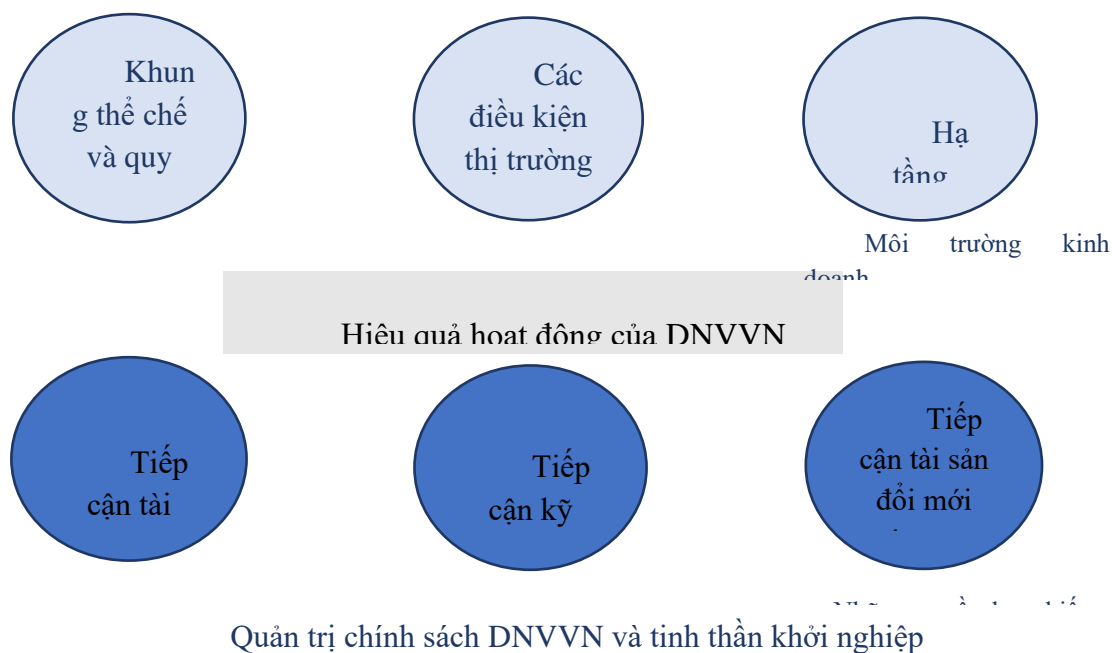
## **1.1. Lợi ích của chuyển đổi số**

Khái niệm chuyển đổi số trong doanh nghiệp khá đa dạng. Theo Verhoef et al. (2021), chuyển đổi số trong doanh nghiệp đòi hỏi phải có nguồn lực, cơ cấu, chiến lược tăng trưởng, các chỉ số và mục tiêu tương ứng với từng giai đoạn cụ thể. Chuyển đổi số là sự kết hợp của các nguồn lực bổ sung vì nó là một quá trình kỹ thuật xã hội. OECD (2017) khẳng định, để ứng dụng thành công CNTT&TT trong DNVVN, thì cần sử dụng tối ưu các tài sản bổ sung dựa vào tri thức như tổ chức và nguồn nhân lực. Các tài sản này cho phép DNVVN giảm lệ thuộc quá mức vào một công nghệ hoặc nền tảng nào đó. Việc không chú trọng đầu tư cho yếu tố con người có thể làm chậm quá trình ứng dụng và phổ biến công nghệ tại các DNVVN.

Ở một khía cạnh khác, Rogers (2016) tin rằng chuyển đổi số về cơ bản không phải là tập trung vào công nghệ, mà là chiến lược. Verhoef et al (2021) đồng tình với quan điểm này và khẳng định thêm rằng chuyển đổi số về bản chất là đa ngành vì quá trình này liên quan đến những thay đổi về chiến lược, tổ chức, CNTT và chuỗi cung ứng, nguồn cung và tiếp thị.

Trong quá trình chuyển đổi số, DNVVN bị tụt hậu, mặc dù đáng lẽ có thể thu được những lợi ích to lớn từ các công cụ, dịch vụ và phương thức số. Số hóa mở ra những cơ hội chưa từng có cho các doanh nghiệp nhỏ vượt qua các rào cản liên quan đến quy mô mà doanh nghiệp thường gặp phải trong quá trình đổi mới để vươn ra toàn cầu và phát triển. Do quy mô hạn chế phạm vi tạo ra lợi thế, nên DNVVN có xu hướng dựa vào sự khác biệt hóa sản phẩm và hiệu ứng mạng và quần tụ (network and agglomeration effect) để cạnh tranh (OECD, 2019).

Hình 1. 6 + 1 trụ cột về hiệu quả hoạt động của DNVVN



Nguồn: OECD (2019[1]), *Tổng quan DNVV và Tinh thần khởi nghiệp 2019*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/34907e9c-en>.

Các công nghệ mới như phân tích dữ liệu lớn, trí tuệ nhân tạo (AI), blockchain và in 3D, cho phép tạo sự khác biệt hóa sản phẩm ở mức cao hơn, cũng như kết hợp hiệu quả giữa các hệ thống chuỗi cung ứng với các mô hình kinh doanh mới nhằm rút ngắn khoảng cách và thời gian đưa sản phẩm ra thị trường. Điều đó đồng thời làm nảy sinh nhu cầu về sản phẩm, đòi hỏi tính linh hoạt và phản ứng mạnh hơn về nguồn cung. Các điều kiện thị trường đang thay đổi này sẽ mang lại lợi ích cho các doanh nghiệp nhỏ và nhạy bén hơn. Trên thực tế, số hóa đã làm thay đổi đáng kể các điều kiện thị trường thông qua giảm quy mô doanh nghiệp hoạt động hiệu quả. Số hóa cho phép giảm chi phí giao dịch liên quan đến các hoạt động thị trường, nghĩa là khả năng tiếp cận thông tin, truyền thông và kết nối, giảm động cơ khuyến khích doanh nghiệp nội bộ hóa các hoạt động đó.

Ngoài ra, số hóa cũng giúp DNVVN hội nhập thị trường toàn cầu, vì giảm chi phí liên quan đến vận tải và hoạt động xuyên biên giới, tăng khả năng thương mại nhiều dịch vụ (trong đó, DNVVN chiếm đa số) và giảm một số chi phí ngầm do chuỗi giá trị toàn cầu (GVC) bị phân khúc gây ra (bổ sung quản lý, logistics và hoạt động).

Số hóa làm thay đổi các điều kiện DNVVN tiếp cận những nguồn lực chiến lược. Số hóa tạo ra rất nhiều dịch vụ tài chính sáng tạo cho các doanh nghiệp



truyền thống gặp khó khăn trong việc tiếp cận nguồn tài chính. Các dịch vụ tài chính từ cho vay ngang hàng (là hình thức cho cá nhân hoặc doanh nghiệp vay thông qua các dịch vụ trực tuyến) đến các công cụ đánh giá rủi ro thay thế. Phát hành tiền ảo lần đầu (ICO) cung cấp tài sản tiền điện tử cũng như các mô hình tài trợ hỗn hợp, đang gia tăng. Fintech (công nghệ tài chính) ngày càng trở thành trung tâm cung cấp tài chính cho DNVVN và những “người chơi lâu năm” trên thị trường sử dụng công cụ Fintech ngày càng nhiều. Số hóa cũng giúp DNVVN dễ tiếp cận các kỹ năng thông qua các nền tảng tuyển dụng việc làm, thuê ngoài và tuyển dụng làm việc trực tuyến hoặc thông qua kết nối họ với các đối tác tri thức.

Số hóa hỗ trợ tạo ra sản phẩm nguồn mở và đổi mới mở, đồng thời tiếp cận nhiều hơn với các tài sản đổi mới sáng tạo như công nghệ, dữ liệu hoặc mạng tri thức. Ví dụ, các công ty đa quốc gia thông qua mạng lưới sản xuất quốc tế, từ lâu đã đóng vai trò là kênh chuyên giao xuyên biên giới “được nội bộ hóa” cho hàng hóa và dịch vụ, dòng tài chính và sở hữu trí tuệ (SHTT). Ngoài ra, các công ty này còn là phương tiện phổ biến các công nghệ số trên toàn cầu. Một số yếu tố như khoảng cách vật lý chi phối phạm vi DNVVN biến đổi quan hệ hợp tác với các công ty đa quốc gia thành lợi ích về năng suất. Số hóa gia tăng có thể làm giảm tầm quan trọng của khoảng cách.

Số hóa cũng đang làm biến đổi khung thể chế. Chính phủ điện tử và các nền tảng trực tuyến đang tạo điều kiện thuận lợi cho việc tham vấn và cung cấp dịch vụ công cho DNVVN. Các ứng dụng kỹ thuật số đã và đang lan rộng trên nhiều lĩnh vực, từ dịch vụ phát triển kinh doanh đến hệ thống li-xăng, tuân thủ thuế.

Song song với đó, nhiều dữ liệu sẵn có kết hợp với nhận thức về hành vi, đang cho phép các nước điều chỉnh dịch vụ theo hướng tốt hơn cho phù hợp với sở thích của người dùng và tạo cơ hội cho việc thử nghiệm chính sách, cải thiện tổng thể hiệu quả của chính sách DNVVN.

## **1.2. Xu hướng phổ biến công nghệ số**

Công nghệ số lan tỏa nhanh nhưng có sự khác biệt giữa các doanh nghiệp, ngành và quốc gia. Phân tích về xu hướng phổ biến công nghệ số chủ yếu được định hướng bởi dữ liệu và dựa vào dữ liệu mới nhất về việc ứng dụng CNTT trong doanh nghiệp, được khai thác từ Cơ sở dữ liệu về Truy cập và Sử dụng CNTT&TT trong doanh nghiệp và Cơ sở dữ liệu Eurostat về Kinh tế số và Xã hội của OECD (OECD, 2020). Đây là kho lưu trữ lớn nhất về các chỉ số so sánh quốc tế về tính kết nối của các doanh nghiệp, khả năng tiếp thu công nghệ số và sự phối hợp của các chuyên gia CNTT&TT. Bộ dữ liệu có sự tham gia của 45 quốc gia châu Âu và OECD (kể cả Braxin) và bao gồm cả dữ liệu có được từ đầu những năm 2000.

*Số hóa doanh nghiệp tiếp diễn mạnh mẽ*

Quá trình số hóa doanh nghiệp tiếp tục diễn ra mạnh mẽ trong những năm gần đây và có sự chênh lệch giữa các quốc gia. Một cuộc thăm dò đầu tiên về sử dụng CNTT&TT, dựa trên tỷ lệ lao động sử dụng máy tính có kết nối Internet, cung cấp một số thông tin chi tiết về mức độ và tốc độ CNTT&TT đã được đưa vào phục vụ hoạt động kinh doanh. Tỷ lệ lao động ở các nước OECD sử dụng máy tính có kết nối Internet, đã tăng đáng kể trong thập kỷ qua. Năm 2019, tỷ lệ này đạt mức trung bình 52%, tăng từ 41% năm 2009. Tuy nhiên, giữa các quốc gia lại có sự chênh lệch lớn, ví dụ, ở Thổ Nhĩ Kỳ chỉ có 24,8% trong khi Thụy Điển lại là 81,7% (2019).

Các doanh nghiệp lớn và nhỏ đều tích cực trang bị nhiều máy tính kết nối Internet cho người lao động, nhưng các doanh nghiệp nhỏ vẫn kém hơn. Tại các nước OECD, kể từ năm 2009, tính trung bình, tỷ lệ lao động trong các doanh nghiệp có từ 10-49 người sử dụng máy tính kết nối Internet, tăng chậm hơn so với các doanh nghiệp khác.

Tất cả các ngành đều đang cung cấp cho người lao động máy tính kết nối Internet, trong đó, một số ngành vượt trội hơn. Trong các dịch vụ cần ứng dụng nhiều kỹ thuật số, việc triển khai sử dụng máy tính kết nối Internet gần như đã hoàn tất. Năm 2019, trung bình 93,6% người làm dịch vụ thông tin và truyền thông và 88,6% người làm dịch vụ chuyên môn, khoa học và kỹ thuật đều sử dụng máy tính kết nối Internet. Dù có nhiều tiến bộ ổn định trong thập kỷ, nhưng vẫn còn các lĩnh vực ít được số hóa như dịch vụ hành chính và hỗ trợ (trung bình 36,2%) và dịch vụ ăn uống và lưu trú (31,8%). Tuy nhiên, việc sử dụng máy tính có Internet đã gia tăng trong các dịch vụ xây dựng (trung bình 45,9%), vận tải và lưu trữ (51,1%), và bán buôn (70,6%) và bán lẻ (70,3%).

### *Số hóa đa khía cạnh*

Số hóa đa khía cạnh liên quan đến việc ứng dụng nhiều loại công nghệ cho các mục đích khác nhau, từ cho phép tiếp cận nhiều hơn với thị trường và người dùng cuối, đến việc tích hợp mạnh mẽ các quy trình kinh doanh hoặc nâng cao năng lực CNTT của doanh nghiệp...

Hệ thống hoạch định nguồn lực doanh nghiệp (ERP) nâng cao hiệu quả và hoạch định chiến lược của bộ phận hành chính. Hệ thống ERP là công cụ phần mềm dùng để quản lý và tích hợp các luồng thông tin nội bộ và bên ngoài, từ nguồn lực vật chất và nhân lực đến tài chính, kế toán và bán hàng, cũng như tự động hóa việc lập kế hoạch, kiểm kê, mua hàng và các chức năng kinh doanh khác.

Công nghệ nhận dạng tần số vô tuyến (RFID) làm tăng hiệu quả sản xuất và logistics. Công nghệ RFID cho phép giao tiếp trường gần, được ứng dụng để: nhận dạng sản phẩm, nhận diện con người hoặc kiểm soát truy cập; giám sát và kiểm

soát sản xuất công nghiệp, chuỗi cung ứng và truy vết hàng tồn kho; quản lý thông tin dịch vụ và bảo trì hoặc cho các ứng dụng thanh toán (như phí cầu đường cao tốc, vận tải hành khách).

Phần mềm Quản lý quan hệ khách hàng (CRM) và Quản lý chuỗi cung ứng (SCM) giúp tăng cường tích hợp bộ phận mũi nhọn của doanh nghiệp và các hoạt động của chuỗi cung ứng. Phần mềm CRM và SCM được sử dụng để quản lý các tương tác của doanh nghiệp với khách hàng, người lao động và nhà cung cấp.

Điện toán đám mây (ĐTĐM) giúp nâng cao năng lực của các hệ thống CNTT. ĐTĐM đề cập đến các dịch vụ CNTT&TT được truy cập qua Internet, bao gồm máy chủ, bộ lưu trữ, các thành phần mạng và ứng dụng phần mềm. ĐTĐM tạo cơ hội cho DN Việt Nam tiếp cận trực tuyến năng lực xử lý hoặc dung lượng lưu trữ bổ sung, cũng như cơ sở dữ liệu và phần mềm, với số lượng phù hợp và theo nhu cầu. Ngoài tính linh hoạt và khả năng mở rộng, ĐTĐM còn giảm chi phí nâng cấp công nghệ vì doanh nghiệp không cần bỏ ra các khoản đầu tư trả trước cho phần cứng và chi phí bảo trì thường xuyên, đội ngũ CNTT và việc chứng nhận. Trên thực tế, tỷ lệ chấp nhận ĐTĐM cao hơn có liên quan đến cường độ đầu tư thiết bị CNTT&TT thấp hơn, các doanh nghiệp đang hướng tới mô hình quản lý CNTT&TT chủ yếu dựa vào việc mua lại phần mềm và kết nối kỹ thuật số.

Phân tích dữ liệu lớn được ứng dụng nhiều trong doanh nghiệp để hỗ trợ tăng hiệu quả của quá trình ra quyết định và lập kế hoạch chiến lược, quản trị chung, sản xuất, tiền sản xuất và logistics hoặc tiếp thị, quảng cáo và thương mại hóa. Phân tích dữ liệu đề cập đến việc sử dụng các kỹ thuật, công nghệ và công cụ phần mềm để phân tích khối lượng lớn dữ liệu bắt nguồn từ các hoạt động được thực hiện bằng phương thức điện tử và thông qua giao tiếp giữa máy với máy.

Mạng xã hội giúp tăng cường nền tảng khách hàng của DN Việt Nam, mở rộng tầm nhìn trong kinh doanh và quảng bá. Mạng xã hội chủ yếu được sử dụng cho các tương tác bên ngoài, bao gồm phát triển hình ảnh và sản phẩm tiếp thị của doanh nghiệp, cũng như thu thập hoặc phản hồi ý kiến, đánh giá và câu hỏi của khách hàng. Mạng xã hội cũng được dùng để kết nối các đối tác kinh doanh hoặc tuyển dụng lao động.

Thương mại điện tử giúp DN Việt Nam củng cố nền tảng khách hàng và nhà cung cấp, tiếp cận các thị trường phi truyền thống trong khu vực hoặc ở nước ngoài. Thương mại điện tử mô tả việc bán hoặc mua hàng hóa hoặc dịch vụ được thực hiện qua mạng bằng các phương thức được thiết kế đặc biệt cho mục đích nhận hoặc đặt hàng (tức là các trang web, extranet (mạng nội bộ) hoặc trao đổi dữ liệu điện tử). Đặt phòng và đặt hàng trực tuyến là các hình thức bán hàng điện tử tiên tiến hơn. Thương mại điện tử diễn ra thông qua một loạt các mối quan hệ thương

mại khác nhau, liên quan đến mọi kết nối giữa người tiêu dùng (C), doanh nghiệp (B) hoặc chính phủ (G). Những kết nối này bao gồm các giao dịch giữa các doanh nghiệp (B2B) cổ điển, vẫn chiếm phần lớn doanh thu từ thương mại điện tử của khu vực tư nhân, cũng như các giao dịch giữa doanh nghiệp với chính phủ (B2G) (ví dụ, mua sắm của chính phủ). Các giao dịch thương mại điện tử ngày càng có sự tham gia trực tiếp của người tiêu dùng, đặc biệt là giao dịch giữa doanh nghiệp với người tiêu dùng (B2C). Ngoài ra, các mô hình kinh doanh mới liên quan đến các mối quan hệ giữa người tiêu dùng với doanh nghiệp (C2B) và quan hệ ngang hàng diễn ra giữa hai hoặc nhiều cá nhân.

Hóa đơn điện tử hỗ trợ các phương pháp tiếp cận tuân thủ theo thiết kế (nghĩa là áp dụng cách tiếp cận có hệ thống để tích hợp các yêu cầu quy định vào các nhiệm vụ và quy trình thủ công và tự động) và giúp tăng cường khả năng tích hợp của hệ thống kế toán và các quy tắc thuế, cuối cùng giảm bớt gánh nặng hành chính cho DNVVN. Lập hóa đơn điện tử hỗ trợ chuỗi thông tin an toàn giữa các doanh nghiệp và cơ quan hành chính công, đồng thời thúc đẩy triển khai các thỏa thuận đóng thuế thu nhập được khấu trừ từ doanh nghiệp và báo cáo cho cơ quan thuế. Ví dụ, hệ thống lập hóa đơn điện tử cho phép cơ quan quản lý thuế bỏ qua các tờ khai thuế thu nhập cá nhân và điền trước đầy đủ các tờ khai thuế thu nhập doanh nghiệp và thuế giá trị gia tăng.

Băng thông rộng tốc độ cao là điều kiện tiên quyết để chuyển đổi số DNVVN. Băng thông rộng cố định tốc độ cao được định nghĩa ở đây là có tốc độ truyền tải ít nhất là 100Mbit/s (nghĩa là cáp quang). Tốc độ truy cập mạng thích hợp là điều cần để khai thác triệt để các dịch vụ hiện có qua Internet và thúc đẩy phổ biến các dịch vụ mới. Sự khác biệt về tốc độ rất quan trọng đối với khách hàng. Ví dụ, thuê bao băng thông rộng tốc độ cao giúp tải một bộ phim chất lượng cao (cỡ 1,5 GB) trong vòng chưa đầy 22 phút, trong khi với thuê bao tốc độ thấp, phải mất ít nhất 52 phút. Do đó, một số chỉ số về sử dụng CNTT trong doanh nghiệp có thể được sử dụng để theo dõi cụ thể hơn việc số hóa một số chức năng kinh doanh của DNVVN (Bảng 1).

Bảng 1. Số hóa các chức năng kinh doanh của DNVVN và các chỉ số sử dụng CNTT trong kinh doanh có liên quan

Chức năng kinh doanh của DNVVN	Chỉ số sử dụng CNTT&TT
Định hướng và hoạch định chiến lược	<ul style="list-style-type: none"> <li>• Doanh nghiệp đã thực hiện phân tích Dữ liệu lớn (%)</li> <li>• Doanh nghiệp sử dụng phần mềm ERP (Quy hoạch nguồn lực doanh nghiệp) (%)</li> </ul>
Quản trị chung và hệ	<ul style="list-style-type: none"> <li>• Doanh nghiệp sử dụng Internet để tương tác với các cơ quan công quyền (%)</li> </ul>

thống CNTT	<ul style="list-style-type: none"> <li>• Doanh nghiệp sử dụng Internet để phát hành/gửi hóa đơn (dạng điện tử hoặc giấy) cho các cơ quan công quyền (%)</li> <li>• Doanh nghiệp mua dịch vụ ĐTĐM (%)</li> </ul>
Sản xuất, tiền sản xuất và logistics	<ul style="list-style-type: none"> <li>• Doanh nghiệp chia sẻ thông tin SCM dưới dạng điện tử với nhà cung cấp và khách hàng (%)</li> <li>• Doanh nghiệp sử dụng công nghệ RFID (%)</li> </ul>
Tiếp thị, quảng cáo và truyền thông	<ul style="list-style-type: none"> <li>• Doanh nghiệp sử dụng mạng xã hội (%)</li> <li>• Doanh nghiệp nhận đơn đặt hàng qua mạng máy tính (%)</li> <li>• Doanh nghiệp có trang web cho phép đặt hàng trực tuyến hoặc đặt trước (ví dụ, qua giỏ hàng) (%)</li> <li>• Doanh nghiệp sử dụng phần mềm CRM (%)</li> </ul>

### *DNVVN có hành trình số hóa cụ thể*

DNVVN tụt hậu trong việc áp dụng công nghệ số. Khoảng cách về tỷ lệ phổ biến công nghệ số của DNVVN so với các doanh nghiệp lớn tồn tại ở tất cả các công nghệ có dữ liệu. Các doanh nghiệp nhỏ vẫn ít được số hóa hơn các doanh nghiệp vừa, còn doanh nghiệp vừa lại không bằng doanh nghiệp lớn. Nhìn chung, các mô hình phổ biến công nghệ của tất cả các loại hình doanh nghiệp đều tương đối giống nhau.

DNVVN có xu hướng số hóa trước hết là trong các hoạt động tiếp thị và quản trị chung. Tỷ lệ tương tác B2G giữa các doanh nghiệp nhỏ, vừa hoặc lớn có sự khác biệt tương đối nhỏ. Tỷ lệ DNVVN chấp nhận mạng xã hội hoặc phần mềm quản lý khách hàng đạt mức cao hơn. Khoảng cách về quy mô doanh nghiệp cũng nhỏ hơn khi doanh nghiệp chuyển sang sử dụng hóa đơn điện tử hoặc tham gia vào thương mại điện tử.

Khoảng cách giữa các DNVVN trong việc áp dụng công nghệ số gia tăng khi các công nghệ ngày càng trở nên tinh xảo. Các doanh nghiệp nhỏ thường ít sử dụng hệ thống ERP hơn các doanh nghiệp lớn. Đó là vì các doanh nghiệp cần có nhiều thời gian, nguồn lực tài chính và nhân lực để triển khai ERP. Do đó, khoảng cách phổ biến ERP giữa DNVVN lớn hơn đáng kể so với giữa các doanh nghiệp vừa và lớn. Điều ngược lại là đúng đối với phần mềm SCM hoặc phân tích dữ liệu lớn mà khoảng cách kỹ thuật số ngày càng nới rộng giữa các doanh nghiệp vừa và lớn. Ngược lại, các doanh nghiệp lớn đã đầu tư nhiều cho việc tích hợp các quy trình kinh doanh của họ (ERP, CRM, SCM), các công cụ lập kế hoạch chiến lược và các công cụ quản lý sản xuất và logistics (RFID).

Các doanh nghiệp lớn đang củng cố hệ thống CNTT thông qua các dịch vụ ĐTĐM bên ngoài. Nhìn chung, mục đích sử dụng đầu tiên mà các doanh nghiệp hướng tới ĐTĐM, là dịch vụ email và dung lượng lưu trữ, sau đó là truy cập vào

phần mềm văn phòng và cơ sở dữ liệu lưu trữ. Tuy nhiên, so với các doanh nghiệp nhỏ thì các doanh nghiệp lớn chủ động hơn trong việc phát triển và bảo trì hệ thống CNTT bên ngoài.

*Sự khác biệt lớn giữa các doanh nghiệp tại nhiều quốc gia về khả năng tiếp cận hạ tầng số*

Giữa các quốc gia có sự khác biệt lớn về cách các doanh nghiệp tiếp cận hạ tầng kỹ thuật số và xây dựng năng lực CNTT. Các nghiên cứu cho thấy lợi ích tiềm năng ngày càng tăng khi các doanh nghiệp áp dụng sớm và lợi ích giảm sau khi phần lớn các doanh nghiệp đã chuyển sang áp dụng công nghệ mới. Ví dụ, ở Đan Mạch và Thụy Điển, hơn một nửa số doanh nghiệp nhỏ được kết nối với băng thông rộng tốc độ cao, điều này khiến các doanh nghiệp kết nối chậm có thể bị giảm lợi ích. Ở Pháp, Hy Lạp hoặc Ý, tỷ lệ này là gần 10% hoặc thậm chí ít hơn. Tương tự như vậy, ở Đan Mạch và Thụy Điển, gần 90% các doanh nghiệp lớn đã kết nối băng thông rộng tốc độ cao. Ở Hy Lạp, Cộng hòa Slovakia và Thổ Nhĩ Kỳ, kết nối sớm là các doanh nghiệp lớn chiếm tỷ lệ gần 35%. Nhìn chung, các doanh nghiệp nhỏ ở Đan Mạch và Thụy Điển kết nối băng thông rộng tốc độ cao nhiều hơn các doanh nghiệp lớn ở Hy Lạp, Cộng hòa Slovakia và Thổ Nhĩ Kỳ. Tình huống tương tự xảy ra khi xem xét các phương thức an ninh kỹ thuật số hoặc mua các dịch vụ ĐTĐM.

Sự khác biệt về hạ tầng số giữa các quốc gia tác động ngày càng lớn đến việc DNVVN áp dụng công nghệ số, khi các giải pháp mới dựa vào ĐTĐM đòi hỏi mạng kỹ thuật số có chất lượng để truyền tải dữ liệu và phương thức an ninh kỹ thuật số mạnh mẽ để bảo vệ mã và hệ thống.

### **1.3. Tác động của đại dịch COVID-19 đến chuyển đổi số**

Từ tháng 2 năm 2020, Trung tâm Nghiên cứu Tinh thần khởi nghiệp, DNVVN, Vùng và Thành phố của OECD đã theo dõi hơn 100 cuộc khảo sát về DNVVN được thực hiện tại 31 quốc gia. Kết quả các khảo sát đã thể hiện quan điểm của DNVVN về tác động của đại dịch COVID-19, nỗ lực ứng phó và kỳ vọng tương lai của DNVVN. Thông tin khảo sát cũng nêu bật tác động của đại dịch COVID-19 đến chuyển đổi số DNVVN.

*70% DNVVN đang sử dụng các công nghệ nhiều hơn do tác động của COVID-19*

Các cuộc khảo sát doanh nghiệp được thực hiện vào năm 2020 trên toàn thế giới cho thấy DNVVN đẩy mạnh tiếp thu công nghệ số và bán hàng trực tuyến từ tháng 5 năm 2020. Kể từ khi đại dịch COVID-19 bùng phát, có đến 70% DNVVN tích cực ứng dụng các công nghệ số, mặc dù có sự khác biệt lớn giữa các quốc gia.

Tuy nhiên, sự khác biệt giữa các DNVVN (đặc biệt là các doanh nghiệp nhỏ) và các doanh nghiệp lớn tiếp tục nói rộng, với mức độ tiếp thu công nghệ số của DNVVN chỉ bằng một nửa so với các doanh nghiệp lớn.

- Khảo sát của Phòng Thương mại Hoa Kỳ diễn ra vào ngày 5 tháng 5, cho thấy xu hướng số hóa đang tăng tốc. Từ tháng 4 đến tháng 5, tỷ lệ doanh nghiệp nhỏ chuyển đổi một phần hoặc toàn bộ lao động sang làm việc trực tuyến, đã tăng từ 12% lên 20%. Số doanh nghiệp nhỏ chuyển sang phương thức kinh doanh bán lẻ với sự hỗ trợ của các phương tiện số, đã tăng từ 10% lên 17%.

- Khảo sát tại 1.128 DNVVN ở Braxin vào tháng 6 cho thấy gần 50% DNVVN đã được “kích hoạt số” mạnh mẽ vào tháng 6 so với trước đại dịch COVID-19. Những cải thiện trong quan hệ khách hàng, cũng như sự nhạy bén của quy trình và khả năng thu hút khách hàng được 55% DNVVN cho là những lợi ích chính của số hóa, tiếp đến là khả năng vận hành từ xa được sự đồng tình của 53,5% DNVVN.

- Nghiên cứu vào tháng 6 của Tập đoàn CISCO về DNVVN ở 8 quốc gia cho thấy 70% DNVVN đang tăng tốc nỗ lực số hóa do COVID-19.

- Nghiên cứu tháng 6 của Ngân hàng Phát triển Kinh doanh Canada đối với 1.000 DNVVN tại quốc gia này cho thấy 21% DNVVN không có ý định thay đổi hoạt động kinh doanh. 60% DNVVN sẽ biến làm việc từ xa thành một phương thức kinh doanh, trong khi 40% DNVVN muốn củng cố tình hình tài chính và tăng đầu tư công nghệ.

- Kết quả khảo sát do Trung tâm Nghiên cứu Hiệu quả kinh tế (CEP)/ Liên đoàn Công nghiệp Anh (CBI) ở Vương quốc Anh thực hiện vào tháng 7 về việc áp dụng công nghệ để ứng phó với đại dịch COVID-19 cho thấy, 75% doanh nghiệp được hỏi đã chuyển sang làm việc trực tuyến. Trong giai đoạn từ cuối tháng 3 đến cuối tháng 7 năm 2020, hơn 60% doanh nghiệp đã áp dụng công nghệ số và phương thức quản lý mới; và khoảng 1/3 doanh nghiệp đầu tư vào năng lực kỹ thuật số mới. Gần một nửa số doanh nghiệp đã giới thiệu sản phẩm hoặc dịch vụ mới.

- Kết quả nghiên cứu vào giữa tháng 7 của công ty Sage (chuyên về các giải pháp quản lý hoạt động kinh doanh ĐTĐM) về việc đặt DNVVN vào trung tâm phục hồi của Vương quốc Anh nêu rõ, 80% DNVVN cho rằng áp dụng kỹ thuật số rất quan trọng đối với sự phục hồi của doanh nghiệp và tạo việc làm, nhưng chỉ một tỷ lệ nhỏ (33%) DNVVN có bằng thông để đầu tư công nghệ trong các quy trình kinh doanh chính.

- Khảo sát của Visa (Mạng lưới thanh toán điện tử) về DNVVN tại 8 quốc gia vào đầu tháng 8 cho thấy 67% DNVVN đã triển khai các bước hướng tới số hóa. Hơn ¼ DNVVN đã thử quảng cáo có mục tiêu trên mạng xã hội hoặc bán sản phẩm hoặc dịch vụ trực tuyến. 20% DNVVN đã áp dụng thanh toán không tiếp xúc và 1/3 DNVVN cho biết đã chấp nhận ít hoặc ngừng chấp nhận tiền mặt.

- Khảo sát vào ngày 19 tháng 8 của GoDaddy (công ty đăng ký và lưu trữ web giao dịch công khai trên Internet của Mỹ) với 5.265 chủ doanh nghiệp nhỏ ở Úc, Canada, Đức, Ấn Độ, Mexico, Philippine, Tây Ban Nha, Thổ Nhĩ Kỳ, Vương quốc Anh và Mỹ cho thấy 40% người được hỏi có trang web doanh nghiệp. Trong số đó, hơn một nửa đã tăng sự “hiện diện trực tuyến” trong đại dịch COVID-19 bằng cách bổ sung nội dung, mở cửa hàng trực tuyến và tăng cường tiếp thị kỹ thuật số. 66% doanh nghiệp Mỹ có khả năng tự xử lý tốt hơn nhu cầu công nghệ, trong khi trên toàn cầu, tỷ lệ này chỉ là 54%. Chỉ 19% doanh nghiệp cho biết đầu tư nhiều hơn cho sự “hiện diện trực tuyến” và 53% doanh nghiệp vẫn giữ nguyên tiền đầu tư này.

- Khảo sát của Allianz (nhà cung cấp dịch vụ tài chính quốc tế) ở Úc vào ngày 27 tháng 8 nêu rõ 20% doanh nghiệp nhỏ đã thay đổi hoàn toàn chính sách trong đại dịch COVID-19 với tỷ lệ 18% tập trung vào số hóa.

- Khảo sát nghiên cứu của American Express (công ty dịch vụ tài chính) cuối tháng 8 cho thấy đối với 24% doanh nghiệp được khảo sát, doanh số bán hàng trực tuyến sẽ chiếm ít nhất một nửa doanh số bán hàng của doanh nghiệp trong năm tới, trong khi 18% doanh nghiệp đã làm được điều đó. 39% doanh nghiệp cho rằng hỗ trợ hữu ích nhất đối với doanh nghiệp trong bối cảnh đại dịch COVID-19 là đào tạo kỹ thuật số.

- Khảo sát của tập đoàn công nghệ Hewlett Packard tại một số quốc gia châu Á - Thái Bình Dương vào đầu tháng 9 cung cấp thông tin về việc áp dụng kỹ thuật số rất quan trọng đối với sự phục hồi của DNVVN và hiện DNVVN đang tập trung quản lý dòng tiền của họ.

- Theo báo cáo khảo sát của công ty phần mềm Salesforce tại Tây Ban Nha (ngày 29 tháng 10), trong đại dịch COVID-19, DNVVN đã lựa chọn các chiến lược tiếp thị kỹ thuật số cho phép tiếp cận khách hàng thông qua các kênh mới này, bất chấp những hạn chế về khả năng di chuyển. 7 trong số 10 doanh nghiệp Tây Ban Nha đã được số hóa để ứng phó với đại dịch COVID-19 và chi cho tiếp thị kỹ thuật số so với tổng ngân sách của doanh nghiệp đã tăng trung bình lên 12,6% ngân sách doanh nghiệp từ tháng 5, mức cao nhất được ghi nhận trong báo cáo, tăng từ 11,3% vào tháng 2.



- Một nghiên cứu vào tháng 11 của công ty Paypall được thực hiện với các doanh nghiệp nhỏ ở Canada về việc đại dịch COVID-19 đã thúc đẩy thương mại kỹ thuật số trong doanh nghiệp, nêu rõ 67% doanh nghiệp nhỏ hiện chấp nhận thanh toán trực tuyến và 47% trong số đó mới bắt đầu trong năm nay. Trong số tất cả các doanh nghiệp nhỏ bán hàng trực tuyến, 34% chỉ chuyển sang thanh toán bằng phương thức số sau khi COVID-19 được tuyên bố là đại dịch toàn cầu vào tháng 3. Đa số các chủ doanh nghiệp nhỏ hoạt động trực tuyến (72%) tin rằng thương mại điện tử hiện nay là cần thiết để kinh doanh thành công. Trên thực tế, 69% chủ doanh nghiệp nhỏ hoạt động trực tuyến cho biết bán hàng trực tuyến giúp họ thành công hơn và nếu không có khả năng này, 58% chủ doanh nghiệp nhỏ cho biết doanh nghiệp của họ sẽ không tồn tại trong bối cảnh đại dịch COVID-19.

- Khảo sát vào ngày 16 tháng 11 của Hewlett Packard (tập đoàn công nghệ thông tin) với 600 doanh nghiệp Việt Nam và 7 quốc gia láng giềng gồm có Úc, Ấn Độ, Indonesia, Nhật Bản, Singapore, Hàn Quốc và Thái Lan cho thấy, DNVVN Việt Nam lạc quan nhất khu vực châu Á - Thái Bình Dương về kịch bản hậu COVID-19. Tại Việt Nam, 41% doanh nghiệp được khảo sát, kỳ vọng sẽ tăng trưởng trong năm tới, trong khi tỷ lệ này của khu vực chỉ là 16%, với 47% trong số đó tin rằng việc áp dụng kỹ thuật số là chìa khóa cho tăng trưởng sau đại dịch.

- Khảo sát vào tháng 12 của KOSGEB, Tổ chức Phát triển DNVVN của Thổ Nhĩ Kỳ, về DNVVN cho thấy 32,6% doanh nghiệp đã chuyển hoạt động kinh doanh sang môi trường kỹ thuật số khi đại dịch xảy đến và 21,8% doanh nghiệp chưa có kế hoạch làm điều đó.

*DNVVN trong các ngành bị ảnh hưởng nhiều nhất đã chuyển đổi hoạt động kinh doanh*

Những ngành bị ảnh hưởng nặng nề nhất bởi đại dịch COVID-19 do những hạn chế về giãn cách xã hội, đứt gãy chuỗi cung ứng và gián đoạn hoạt động. Đây cũng là những ngành mà phương thức làm việc từ xa và sắp xếp làm việc thông minh hoặc các giải pháp kỹ thuật số không dễ thực hiện. Nhìn chung, các ngành này cung cấp từ 35-45% tổng số việc làm tại các nước OECD.

Thương mại điện tử đã trải qua những cú sốc về cả nguồn cung và cầu. Khi mọi người tránh đám đông và các trung tâm mua sắm do đại dịch COVID-19, các cửa hàng bán lẻ phải đóng cửa, người tiêu dùng đã chuyển sang lựa chọn giao hàng tận nhà. Doanh số bán hàng điện tử đã tăng lên trên toàn thế giới nhưng không đồng đều giữa các dòng sản phẩm. Rất nhiều đơn đặt hàng thực phẩm, hàng tiêu dùng thiết yếu hoặc đồ gia dụng và thiết bị (như máy in hoặc tủ lạnh), trong khi nhu cầu đối với các sản phẩm bán trực tuyến truyền thống hàng đầu (như quần áo hoặc đồ điện tử) chỉ hạn chế. Ngược lại, người bán trên thị trường kỹ thuật số có

sự chậm trễ trong việc giao hàng hoặc cung cấp không thành công, do gián đoạn lớn trong chuỗi logistics và hệ thống vận tải.

- Hiệu bánh Circus, một DNVVN của Pháp, đã ra mắt trang web bán lẻ 24 giờ sau khi đóng cửa hàng duy nhất. Trang web cung cấp dịch vụ giao hàng và dịch vụ “click & collect” (đặt hàng trực tuyến và đến cửa hàng lấy), cho phép tiệm bánh tiếp tục hoạt động trong thời kỳ khủng hoảng.

- Five Way Cellars, nhà bán lẻ rượu của Úc, đã khai trương trang web bán lẻ vào năm 2019, sau 30 năm hoạt động để bổ sung cho các hoạt động bán hàng trực tiếp tại cửa hàng. Trong thời gian phong tỏa do COVID-19, Five Way Cellars đã sử dụng nền tảng số này làm nguồn kinh doanh chính. Lần đầu tiên, thương hiệu này tham gia vào mạng xã hội (Instagram, Facebook) để quảng bá sản phẩm nhằm nỗ lực cạnh tranh với các nhà phân phối lớn có chiết khấu giá cao.

- Natoora, nhà bán buôn nông sản tươi sống của Vương quốc Anh, đã thay đổi hoàn toàn mô hình kinh doanh từ doanh nghiệp với doanh nghiệp (B2B) sang doanh nghiệp với người tiêu dùng (B2C), vì không thể duy trì các hoạt động bán buôn cho các nhà hàng và doanh nghiệp, trong đó, nhiều nơi đã phải đóng cửa do các hạn chế giãn cách. Thông qua trang web mới, doanh nghiệp đã đưa sản phẩm đến với các hộ gia đình và khách hàng cá nhân.

Ngành công nghiệp giải trí đã phát triển các thị trường mới để ứng phó với giãn cách xã hội. Các lớp học khiêu vũ, thư giãn hoặc nấu ăn đang chuyển sang hình thức trực tuyến. Các bảo tàng đang tổ chức các chuyến tham quan thực tế ảo. Các nhà cung cấp dịch vụ phát trực tuyến video và truy cập Internet đã tăng số lượt đăng ký thông qua đề xuất quyền truy cập miễn phí vào TV theo yêu cầu hoặc các dịch vụ trực tuyến miễn phí.

- SkyTing Yoga là phòng tập yoga đặt tại New York. Trước đó vào năm 2020, đơn vị này đã công bố nền tảng kỹ thuật số “SkyTing TV” như một dịch vụ bổ sung. Đây đã trở thành nguồn doanh thu chính của doanh nghiệp cùng với một dịch vụ mới phát trực tuyến các lớp học qua Instagram để quyên góp thông qua nền tảng thanh toán Venmo.

- Boiler Room, công ty sản xuất âm nhạc và tổ chức sự kiện, thay vì hủy 40 buổi hòa nhạc sắp tới, đã phát trực tiếp các sự kiện qua nền tảng Internet từ nhà riêng và không gian riêng của các nghệ sĩ.

Ngành ngân hàng điện tử và thanh toán di động đã thích nghi với các điều kiện thị trường mới, trong khi các doanh nghiệp buộc phải chuyển sang bán hàng trực tuyến, thì người tiêu dùng và doanh nghiệp tìm kiếm các giải pháp để tránh tiếp xúc với tiền giấy (một số cửa hàng chỉ thanh toán bằng thẻ tín dụng). Các

ngân hàng thương mại khuyến khích khách hàng sử dụng các dịch vụ ngân hàng trực tuyến dựa trên ứng dụng.

Dịch vụ học trực tuyến đã có sức lan tỏa rộng rãi. Các hệ thống giáo dục đã ồ ạt chuyển sang học trực tuyến, vì hơn 900 triệu trẻ em và thanh thiếu niên tại hơn 102 quốc gia đã phải ở nhà vì trường học bị đóng cửa do lệnh phong tỏa. Các trường đại học lớn đã hủy bỏ các lớp học trực tiếp để chuyển sang đào tạo trực tuyến. Trong một thời gian rất ngắn, các phương pháp học tập có sự hỗ trợ kỹ thuật số, đã trở thành giải pháp thay thế tạm thời cho các phương pháp học truyền thống trực tiếp. Sự thay đổi của kỹ thuật số cũng đã ảnh hưởng đến các dịch vụ giáo dục kinh doanh.

Các giải pháp làm việc thông minh đã nở rộ để giải quyết tình trạng biến mất gần như hoàn toàn của các hoạt động kinh doanh trực tiếp và tại chỗ. Việc hủy bỏ các triển lãm và hội nghị thương mại đã đặt ra thách thức lớn đối với các doanh nghiệp sử dụng các kênh B2B để xây dựng mạng lưới chuyên nghiệp và thu hút khách hàng mới. Điều này đặc biệt đúng với các doanh nghiệp nhỏ dựa vào phương thức truyền miệng và danh tiếng để thiết lập mạng lưới. Một số doanh nghiệp số lớn và cả DNVVN đã triển khai áp dụng một loạt các giải pháp kỹ thuật số. Dưới đây là một số ví dụ từ cuộc gọi thoại và video đến hội nghị từ xa, hội thảo trên web phát trực tiếp và làm việc từ xa:

- Công ty IBM tổ chức hội nghị khách hàng và nhà phát triển “Think 2020” và hội nghị đối tác “PartnerWorld” với tư cách là các sự kiện số toàn cầu bằng cách kết hợp nội dung phát trực tiếp, các phiên họp tương tác và các sự kiện được tổ chức tại địa phương.

- Google đã thay đổi sự kiện Cloud Next thành hội nghị số trong năm nay.

- Wolf PR, DNVVN trong lĩnh vực truyền thông và quảng cáo của Israel, đã triển khai chính sách làm việc tại nhà cho nhóm gồm 20 người. Trong khi làm việc từ xa, người lao động sử dụng nền tảng hội nghị từ xa Zoom để giữ kết nối và nền tảng đám mây của Microsoft Office để chia sẻ thông tin.

- Hylton and Company Realty là DNVVN chuyên về bất động sản tại Hoa Kỳ. Phần lớn hoạt động kinh doanh đã chuyển sang phương thức kỹ thuật số, thông qua một trang web là điểm liên hệ chính của khách hàng. Để đối phó với thách thức làm việc tại nhà, “ngôi nhà mở” đã được giới thiệu trực tuyến bằng cách camera, chuyến tham quan ảo và video quay từ máy bay không người lái để hiển thị các thuộc tính.

Đặc biệt, một số doanh nghiệp đã thay đổi hoàn toàn mô hình kinh doanh với sự trợ giúp của các công cụ kỹ thuật số.

- Older, loại hình doanh nghiệp dệt may nhỏ và vừa chuyên sản xuất đồng phục cho khách sạn, đã phản ứng với sự sụt giảm nhu cầu bằng cách thay đổi mô hình kinh doanh chuyển sang sản xuất khẩu trang. Doanh nghiệp này đã sử dụng trang web và Instagram để xử lý các đơn đặt hàng.

- Pepe's Sydney, một nhà hàng ở Úc, đã phản ứng với các hạn chế của COVID-19 bằng cách thay đổi mô hình kinh doanh, từ nhà hàng ăn uống cao cấp sang dịch vụ bán hàng mang đi bằng các nền tảng giao hàng như Uber Eats.

#### **1.4. Chính sách hỗ trợ chuyển đổi số cho doanh nghiệp vừa và nhỏ**

Sự tụt hậu về mặt kỹ thuật số của DNVVN xuất phát từ rất nhiều yếu tố và rào cản, bao gồm cả việc DNVVN thiếu thông tin và nhận thức, thiếu kỹ năng, không đủ vốn hoặc thiếu tài sản bổ sung như công nghệ hoặc thực tiễn tổ chức. Các doanh nghiệp nhỏ thường gặp nhiều khó khăn khi thích ứng với sự thay đổi của khung pháp lý, đối phó với các vấn đề về an ninh và bảo mật số hoặc chỉ đơn giản là truy cập hạ tầng kỹ thuật số hiện đại.

Các quốc gia OECD tập trung đẩy mạnh phổ biến đổi mới kỹ thuật số cho DNVVN và đảm bảo khả năng bắt kịp quá trình chuyển đổi số. Tuy nhiên, rất nhiều phương pháp và trong một số lĩnh vực là các quan điểm khác nhau về cách phát huy tiềm năng kỹ thuật số của DNVVN và chủ doanh nghiệp, lý giải sự không đồng nhất lớn giữa các DNVVN và sự đa dạng của hệ sinh thái kinh doanh. Trong khi một số quốc gia đã tìm cách lồng ghép các cân nhắc chính sách về DNVVN trong các chương trình chính sách khác, thì các quốc gia khác lại nhắm mục tiêu cụ thể đến các DNVVN bằng các công cụ được thiết kế riêng, thường được kết hợp với hỗn hợp chính sách đặc thù cho ngành hoặc vùng.

##### *Hỗ trợ công nghệ cho DNVVN*

Chủ doanh nghiệp nhỏ thường không biết về các công cụ số mới tiềm năng giúp cải thiện hoạt động kinh doanh hoặc họ coi chi phí trả trước của việc nâng cấp hướng tới công nghệ kỹ thuật số tinh xảo là quá cao.

Các nhà hoạch định chính sách đã tích cực cung cấp hỗ trợ tài chính và kỹ thuật để DNVVN tiến hành chẩn đoán công nghệ và giải quyết vấn đề hoặc triển khai các giải pháp kinh doanh điện tử mới, thường dưới dạng các sáng kiến quy mô nhỏ và tại chỗ. Trong một số trường hợp, hỗ trợ tài chính và kỹ thuật được bổ sung cho đào tạo và hướng dẫn thay đổi tổ chức và bộ kỹ năng cần thiết để hỗ trợ thay đổi công nghệ.

Các chương trình mở rộng công nghệ do chính phủ tài trợ nhằm tăng khả năng tiếp thu và thích ứng với các công nghệ hiện có (như thiết bị, kỹ năng quản lý mới) trong các doanh nghiệp. Mặc dù hình thức hỗ trợ này không phải là mới, nhưng

việc sử dụng các chương trình mở rộng công nghệ nhằm vào DNVVN đã được tăng cường trong những thập kỷ qua.

#### Hộp 1. DNVVN và các chương trình mở rộng công nghệ

Các chương trình mở rộng công nghệ thường bắt đầu bằng việc đánh giá các hoạt động và quy trình của doanh nghiệp, sau đó là một kế hoạch được đề xuất để cải tiến và hỗ trợ thực hiện. Các dịch vụ chính bao gồm cung cấp thông tin (để cải thiện việc áp dụng các công nghệ, xu hướng, phương thức tốt nhất hiện có); đưa ra tiêu chuẩn để xác định các lĩnh vực cần cải tiến; hỗ trợ kỹ thuật và tư vấn; và đào tạo.

Các dịch vụ mở rộng công nghệ thường được cung cấp bởi mạng lưới các chuyên gia kỹ thuật (ví dụ, kỹ sư), chủ động liên hệ với các doanh nghiệp để tổ chức các chuyến thăm và tham vấn. Tuy nhiên, các doanh nghiệp cũng có thể liên hệ để được hỗ trợ về các chương trình mở rộng công nghệ.

Loại hình hỗ trợ này thường được cung cấp riêng cho các doanh nghiệp quan tâm, nhưng cũng có thể được cung cấp đồng thời cho các nhóm doanh nghiệp có nhu cầu chung. Các giai đoạn xem xét và phán đoán đầu tiên thường miễn phí, trong khi các dự án chuyên sâu hơn thường yêu cầu doanh nghiệp đồng tài trợ, mặc dù với giá dịch vụ tư vấn thấp hơn giá thị trường.

Như một phần trong các hoạt động ứng phó với cuộc khủng hoảng COVID-19, các quốc gia đã tăng cường nỗ lực hướng tới số hóa DNVVN, thông qua các kế hoạch mới hay củng cố các kế hoạch cũ. Ngoài ra, một số quốc gia đã phải điều chỉnh khung pháp lý và quy định để tạo môi trường triển khai dàn xếp làm việc theo phương thức mới và các mô hình kinh doanh. Chile đã sửa đổi Bộ luật Lao động để điều chỉnh hoạt động làm việc từ xa.

Bảng 2. Các chương trình hỗ trợ công nghệ: ví dụ từ các quốc gia

Quốc gia	Sáng kiến	Mô tả
Hỗ trợ tài chính		
Argentina	Phản ứng COVID-19	Tài trợ 7,2 triệu EUR cho DNVVN làm việc từ xa.
Đan Mạch	DNVVN: Số hóa (2018-2021)	Hỗ trợ tài chính trực tiếp nhằm cải thiện việc tiếp thu công nghệ số và thương mại điện tử giữa các DNVVN.
Estonia	Tài trợ số hóa (2019)	Hỗ trợ tài chính cho triển khai các công nghệ số và rô bốt, cũng như tự động hóa trong ngành sản xuất và khai thác mỏ.
Israel	Khuyến khích thuế thúc đẩy đầu tư	Cung cấp tín dụng thuế hoặc khấu hao đặc biệt cho đầu tư CNTT tiên tiến để thúc đẩy tăng

Quốc gia	Sáng kiến	Mô tả
	CNTT (2018-2020)	trưởng như một phần của Cách mạng công nghiệp 4.0 và tăng cường sử dụng rộng rãi các công cụ số.
Ai-len	Phiếu mua hàng trực tuyến	Trong bối cảnh COVID-19, chương trình được cấp thêm 3,3 triệu EUR, theo đó, các doanh nghiệp siêu nhỏ có thể nhận được phiếu mua hàng trị giá 2.500 EUR để phát triển hoạt động bán hàng online và tiếp cận đào tạo trực tuyến miễn phí.
Nhật Bản	Đầu tư vốn để cách mạng hóa năng suất cho DNVVN (2018)	Hỗ trợ DNVVN và doanh nghiệp siêu nhỏ đầu tư vốn thông qua các tổ chức hỗ trợ đã được phê duyệt nhằm phát triển các dịch vụ sáng tạo, sản xuất nguyên mẫu, cải tiến quy trình sản xuất và giới thiệu các công cụ CNTT để tăng năng suất.
	Phản ứng với COVID-19	Trợ cấp hỗ trợ DNVVN làm việc từ xa áp dụng các giải pháp CNTT và phát triển các kênh bán hàng thương mại điện tử.
Bồ Đào Nha	Phiếu mua hàng công nghiệp 4.0 (2017)	Chương trình tài trợ cho DNVVN đang tìm cách triển khai hoạt động trong các lĩnh vực như thương mại điện tử, tiếp thị trực tuyến, phát triển và bảo trì trang web, dữ liệu lớn...
Slovenia	Phiếu kỹ thuật số	Hỗ trợ DNVVN 10.000 EUR để nâng cao năng lực số, chuẩn bị chiến lược số, cho phép an ninh mạng triển khai tiếp thị kỹ thuật số.
Tư vấn, thông tin và hỗ trợ phi tài chính		
Chile	Số hóa DNVVN (Digitaliza tu Pyme) (2019-2021)	Cung cấp gói công cụ số và tài liệu học tập cho các doanh nghiệp nhỏ để tăng doanh số bán hàng, giảm chi phí hoạt động và cải thiện quan hệ với khách hàng và nhà cung cấp bằng các công nghệ số. Chương trình được tăng cường trong bối cảnh COVID-19.
Đức	Số hóa (2017-2021)	Hỗ trợ DNVVN (dưới 100 lao động và có tổng bảng cân đối kế toán lên đến 20 triệu EUR) trong các lĩnh vực bảo mật CNTT, số hóa quy trình kinh doanh và phát triển thị trường kỹ thuật số, dựa vào tư vấn chuyên môn từ các công ty tư vấn được ủy quyền hỗ trợ các doanh nghiệp trong toàn bộ quá trình này.
	Chương trình doanh	Chương trình nhằm tăng cường số hóa các doanh

Quốc gia	Sáng kiến	Mô tả
Hungary	ngành hiện đại - Tinh thần khởi nghiệp số (2015-2021)	ngành nông thôn với sự trợ giúp của 27 chuyên gia tư vấn CNTT.
Litva	Tư vấn Kinh doanh LT (2014 - 2023)	Mục tiêu là tư vấn phát triển kinh doanh cụ thể ở cấp cao cho các doanh nghiệp Litva.
Malaysia	Tập đoàn kinh tế số	Do chính phủ thành lập như một phần của chiến lược số quốc gia và được huy động trong cuộc khủng hoảng COVID-19 để cung cấp danh mục đầy đủ các giải pháp kỹ thuật số cho DNVVN thông qua các công ty công nghệ Malaysia.
Bồ Đào Nha	Opendays i4.0 (từ 2018)	Chiến dịch nâng cao nhận thức nhằm thúc đẩy nhu cầu chuyển đổi số trong DNVVN.
<b>Kết hợp các biện pháp hỗ trợ (tài chính và phi tài chính)</b>		
Úc	Dịch vụ tư vấn doanh nghiệp nhỏ ở Úc (ASBAS) (2018-2021)	Cung cấp hỗ trợ trực tiếp (trợ cấp) và phi tài chính (dịch vụ tư vấn) cho các doanh nghiệp nhỏ. Từ tháng 11/2020, các doanh nghiệp mới tiếp cận dịch vụ này sẽ được đánh giá ban đầu về nhu cầu và được cấp quyền truy cập vào hội thảo trên web và tư vấn 1-1.
	Nhà vô địch kỹ thuật số là doanh nghiệp nhỏ (2019-2021)	Với ngân sách 8,9 triệu AUD, chương trình nhằm đẩy mạnh tương tác giữa các doanh nghiệp số nhỏ và các nhà lãnh đạo hoặc nhà đổi mới nổi tiếng ở Úc thông qua tài trợ trực tiếp và dịch vụ theo dõi (tư vấn).
Columbia	Thúc đẩy chuyển đổi số các doanh nghiệp Colombia (2019 - 2022)	Tăng mức độ áp dụng các công nghệ mới và chín muồi: (i) thay đổi tinh thần và văn hóa kinh doanh; (ii) hỗ trợ chuyển đổi các quy trình kinh doanh; và (iii) đẩy mạnh phát triển và áp dụng công nghệ chuyển đổi số trong doanh nghiệp.
	Chính sách kinh tế số (2015)	Tạo ra tăng trưởng kinh tế nhanh chóng thông qua hỗ trợ các doanh nghiệp và áp dụng CNTT&TT.
Nga	Chương trình số hóa và chuyển đổi số DNVVN	Bao gồm các biện pháp bổ sung khác nhau như phiếu kỹ thuật số (digital voucher), dịch vụ tư vấn và nâng cao kỹ năng để cải thiện quyền truy cập và sử dụng các công cụ số.
Thụy Điển	Robo-Lift (2019-	Hỗ trợ tự động hóa DNVVN ở Thụy Điển. Thông qua Robo-Lift, DNVVN được hỗ trợ tài

Quốc gia	Sáng kiến	Mô tả
	2021)	chính, tiếp cận đào tạo và tham gia kết nối với các bài tập về vấn đề tự động hóa.
Với cách tiếp cận theo ngành hoặc tập trung vào công nghệ		
Colombia	Phòng thí nghiệm Khu vực kỹ thuật số và Thương mại điện tử cạnh tranh hơn (2019-2022)	Thúc đẩy việc thông qua và áp dụng công nghệ trong các ngành sản xuất và trong các doanh nghiệp là một phần của chuỗi giá trị thương mại điện tử.
Estonia	Hội thảo chuyên đề về giải pháp kỹ thuật số cho ngành công nghiệp (từ 2017)	Sáng kiến này bao gồm các hội thảo chuyên đề và các phiên họp kết nối.
Nhật Bản	Áp dụng dịch vụ đám mây cho DNVVN (từ 2015)	Mục tiêu chính của sáng kiến là mở rộng thị trường dịch vụ đám mây
Hà Lan	Chiến lược số hóa Hà Lan (từ 2018)	Thúc đẩy quá trình chuyển đổi số trong các ngành được lựa chọn (chăm sóc sức khỏe, vận tải, giáo dục, năng lượng và lĩnh vực nông sản).
Bồ Đào Nha	Bồ Đào Nha i4.0, Chiến lược quốc gia số hóa nền kinh tế	Sáng kiến i4.0 của Bồ Đào Nha là chiến lược của chính phủ nhằm số hóa ngành công nghiệp.
Thụy Điển	Digi-lift (2016-2019)	Digi-Lift kích thích chuyển đổi số trong doanh nghiệp với trọng tâm là ngành công nghiệp. Digi-Lift là một phần của Smart Industry - chiến lược công nghiệp của Thụy Điển. Digi-Lift mang đến cho các doanh nghiệp khả năng tương tác với các bên liên quan của quá trình chuyển đổi số để nhận được các dịch vụ tư vấn và huấn luyện.

*Nguồn: Phản ứng của các quốc gia trong Khảo sát Tổng quan kinh tế số của OECD về việc tiếp thu các công nghệ số của doanh nghiệp năm 2019 và OECD (2020[6]), “Coronavirus (COVID-19): SME policy responses”, OECD Policy Responses to Coronavirus (COVID-19), [www.oecd.org/coronavirus/policy-responses/coronavirus-covid-19-sme-policy-responses-04440101/](http://www.oecd.org/coronavirus/policy-responses/coronavirus-covid-19-sme-policy-responses-04440101/).*

### *Khuyến khích DNVVN đào tạo và nâng cao kỹ năng*

DNVVN thường khó thu hút và giữ chân lao động lành nghề hơn so với các doanh nghiệp lớn vì DNVVN có xu hướng thiếu năng lực và mạng lưới để xác định và tiếp cận nhân tài và đặc biệt là mức lương và điều kiện làm việc kém hấp



dẫn. Bên cạnh đó, DNVVN cung cấp ít cơ hội đào tạo và phát triển lao động, thường là do thiếu các bộ phận đào tạo nội bộ hoặc bộ phận nhân sự để tổ chức và phối hợp đào tạo, và các kỹ năng quản lý dự báo nhu cầu còn hạn chế. Ngoài ra, chi phí đào tạo phù hợp tương đối cao đối với DNVVN vì họ có ít lao động để phân bổ chi phí đào tạo cố định. Hơn nữa, DNVVN thường có tốc độ thay thế lao động cao hơn, hạn chế năng lực và sự sẵn sàng của doanh nghiệp trong việc đầu tư phát triển kỹ năng cho người lao động, bởi một lao động lành nghề có nguy cơ sẽ rời đi ngay sau khi được đào tạo.

#### *Thu hút DNVVN vào hoạt động giáo dục và đào tạo*

Một số loại hình sáng kiến chính sách có thể được triển khai để hỗ trợ phát triển kỹ năng của lực lượng lao động trong DNVVN, chủ yếu tập trung vào giảm chi phí đào tạo cho doanh nghiệp và gia tăng lợi ích của việc đào tạo tại nơi làm việc.

Nhiều quốc gia OECD đưa ra các ưu đãi thuế để giảm chi phí đào tạo cho người lao động mà doanh nghiệp phải bỏ ra. Chi phí đào tạo có thể được khấu trừ một phần hoặc toàn bộ vào lợi nhuận hàng năm của doanh nghiệp dưới hình thức miễn thuế. Các chương trình này có thể hướng cụ thể đến các doanh nghiệp nhỏ thông qua cung cấp các khoản khấu trừ bổ sung. Các doanh nghiệp nhỏ cũng thường xuyên được hỗ trợ từ các chương trình trợ cấp đào tạo trực tiếp. Ví dụ: phiếu đào tạo giúp DNVVN mua các khóa đào tạo của các cá nhân hoặc tổ chức được công nhận.

Các quốc gia đặt mục tiêu nâng cao nhận thức về tầm quan trọng của đào tạo và phát triển kỹ năng trong DNVVN thông qua nhiều kênh khác nhau, bao gồm cả các tổ chức công và các bên liên quan. Một lựa chọn là tận dụng mạng lưới người sử dụng lao động địa phương để đẩy mạnh việc nâng cao kỹ năng tại nơi làm việc. Các mạng lưới và hiệp hội người sử dụng lao động có thể xúc tiến mối quan hệ dựa vào sự tin cậy giữa các doanh nghiệp để hỗ trợ chia sẻ tri thức và đầu tư chung cho đào tạo. Hợp tác giữa các doanh nghiệp cũng có thể làm tăng sự lan tỏa theo hướng sáng tạo trong chuỗi cung ứng của khu vực, đưa các doanh nghiệp vào chuỗi giá trị toàn cầu, làm giảm tác động đến tự động hóa trong khu vực.

Các quốc gia cũng đang đầu tư nhiều cho các đơn vị “môi giới” hoặc trung gian như các nhóm hoặc văn phòng đào tạo tập thể để tổ chức đào tạo cho các nhóm DNVVN nhằm loại bỏ gánh nặng đào tạo cho người sử dụng lao động. Các tổ chức này thường ký hợp đồng học việc với chính phủ đồng thời cung cấp dịch vụ hỗ trợ thiết thực cho người học. Điều đó đặc biệt hữu ích cho DNVVN không thể đáp ứng các tiêu chuẩn tối thiểu của quốc gia về đào tạo người học nghề và đảm bảo các tiêu chuẩn về chất lượng đào tạo.

Cuối cùng, quy định có thể khuyến khích phát triển kỹ năng. Một số quốc gia đã đưa ra các quyền pháp định đối với lao động khi nghỉ đào tạo. Tuy nhiên, mức độ tuân thủ nhìn chung không cao (dưới 2% lao động được hưởng lợi từ biện pháp này).

### *Tăng cường kỹ năng quản lý trong DNVVN*

Các nước có một số công cụ để xây dựng kỹ năng quản lý trong DNVVN, từ việc cung cấp các công cụ chẩn đoán kỹ thuật số giúp DNVVN xác định những thiếu sót trong quản lý, đào tạo và hội thảo và các phương pháp chuyên sâu hơn như huấn luyện quản lý. Hầu hết các chương trình và sáng kiến thường bao gồm chiến lược kinh doanh, mô hình hoạt động, quản lý quy trình, quản lý hiệu suất, lãnh đạo, quản trị, tính nhạy bén và đổi mới. Một phần quan trọng của kỹ năng quản lý là lập kế hoạch và quản lý tài chính, bao gồm khả năng tiến hành lập kế hoạch rủi ro và cung cấp thông tin tài chính liên quan trong các kế hoạch kinh doanh và dự án đầu tư. Một trong những thách thức lớn đối với các quốc gia là tạo ra nhu cầu về các dịch vụ hỗ trợ hiện có vì nhiều chương trình có tỷ lệ tiếp nhận thấp do thiếu nhận thức về các chương trình hiện có; các vấn đề về tính hợp pháp xoay quanh các nhà điều hành hỗ trợ công; nghi ngờ về tính hữu dụng của việc tư vấn; và tham vọng hạn chế trong phát triển và tăng trưởng kinh doanh.

*Bảng 3. Ví dụ về các chương trình phát triển kỹ năng của một số quốc gia*

Quốc gia	Sáng kiến	Mô tả
Colombia	Trung tâm Xuất sắc và Phân bổ (2019-2022)	Cung cấp các khóa đào tạo liên tục hoặc ngắn hạn của các chuyên gia về các công nghệ mới như Dữ liệu lớn và Internet kết nối vạn vật (IoT) nhằm đưa ra các giải pháp công nghệ có thể tác động đến quá trình chuyển đổi số của các ngành sản xuất trong nước.
Đức	Số hóa (2017-2021)	Hỗ trợ DNVVN (dưới 100 lao động và có tổng bảng cân đối kế toán lên đến 20 triệu EUR) trong các lĩnh vực bảo mật CNTT, số hóa quy trình kinh doanh và phát triển thị trường kỹ thuật số, dựa vào tư vấn chuyên môn từ các công ty tư vấn được ủy quyền hỗ trợ các doanh nghiệp trong toàn bộ quá trình.
Israel	Đào tạo CNTT&TT cho DNVVN (2014)	Đào tạo CNTT&TT cho DNVVN để cải thiện hoạt động kinh doanh và tăng năng suất.
Latvia	Hỗ trợ đào tạo người lao động (2014-2020)	Hỗ trợ nâng cao kỹ năng cho người lao động Latvia dù họ thuộc doanh nghiệp quy mô nào.

Tây Ban Nha	Chương trình Acelera PYME	Trong bối cảnh COVID-19, hỗ trợ DNVVN và người tự doanh suy nghĩ lại về mô hình kinh doanh của họ và củng cố các kỹ năng quản lý và kỹ thuật số.
Anh	Chương trình lãnh đạo doanh nghiệp nhỏ ở Anh (từ 2018)	Đào tạo quản lý cho 2.000 lãnh đạo doanh nghiệp nhỏ trong năm đầu tiên với mục tiêu mở rộng quy mô lên đến 10.000 người vào năm 2025. Gói các biện pháp này nhằm hỗ trợ các doanh nghiệp cải thiện năng suất, bao gồm tăng cường các mạng lưới địa phương, thu hút các doanh nghiệp đã đăng ký các chương trình tư vấn và thúc đẩy “Hợp tác Chuyên gia tri thức”, theo đó, nghiên cứu sinh được đưa vào các doanh nghiệp để biến những nội dung nghiên cứu thành tăng trưởng kinh doanh.

### *Khai thác Fintech và các nguồn tài chính thay thế dành cho DNVVN*

Trong tất cả các giai đoạn của vòng đời, DNVVN phải đối mặt với các rào cản cơ cấu trong việc tiếp cận các nguồn tài chính phù hợp cần cho đổi mới sáng tạo và tăng trưởng. Các rào cản nội bộ bao gồm thiếu tài sản thế chấp cho các nhà tài trợ và nhà đầu tư, thiếu kỹ năng tài chính của các chủ doanh nghiệp nhỏ và nhà quản lý, thiếu kiến thức và nhận thức về các giải pháp tài trợ và những lựa chọn thay thế. Các rào cản thị trường bao gồm sự mất cân đối về thông tin giữa các tổ chức tài chính và ban quản lý DNVVN, chi phí giao dịch và vay tương đối cao của các tổ chức tài trợ tính cho DNVVN. Những thách thức trên thường thể hiện rõ nét ở nhóm doanh nghiệp mới, công ty khởi nghiệp và các dự án đổi mới có tiềm năng tăng trưởng cao tại các vùng sâu vùng xa và nông thôn hoặc các doanh nghiệp được lãnh đạo bởi phụ nữ, thanh niên, người cao tuổi và người di cư.

Hoạt động tài chính thay thế trực tuyến được lồng ghép nhiều vào các chính sách tài chính của DNVVN. Sử dụng các công nghệ như xác minh ID kỹ thuật số, công nghệ sổ cái phân tán (DLT), dữ liệu lớn và cho vay trên sàn giao dịch (marketplace lending), các nhà cung cấp tài chính đang đưa ra rất nhiều dịch vụ sáng tạo với tiềm năng cách mạng hóa thị trường tài chính của DNVVN. Ngân hàng di động, thanh toán di động (quốc tế) và sử dụng dữ liệu thay thế để đánh giá rủi ro tín dụng có thể làm giảm đáng kể sự bất cân xứng về thông tin và chi phí giao dịch, dỡ bỏ các rào cản cấu trúc của DNVVN trong việc tiếp cận tài chính.

Fintech, được định nghĩa là đổi mới được hỗ trợ bởi công nghệ trong các dịch vụ tài chính, ngày càng quan trọng hơn trong việc cung cấp các dịch vụ tiện lợi và

đề tiếp cận, đánh giá rủi ro tín dụng hiệu quả và chi phí giao dịch thấp hơn. Những công cụ này có thể mang lại cơ hội duy nhất cho các dự án quá nhỏ, quá rủi ro hoặc nhằm mục đích xã hội và đặc biệt việc mở rộng mạnh mẽ của các công cụ này vào đầu những năm 2010 đã khiến các nhà quản lý phải can thiệp.

Để xác định các phương thức hiệu quả thực hiện các Nguyên tắc cấp cao của G20/OECD về Tài trợ cho DNVVN, phần lớn các quốc gia đều ủng hộ phát triển các giải pháp Fintech (27/38). Các sáng kiến quản lý bao gồm 19 trong số 27 giải pháp này. Ngoài ra, các nền tảng thông tin và kết nối DNVVN với các công ty Fintech, hội thảo và thành lập hiệp hội Fintech cũng đã được đề cập.

Đại dịch COVID-19 đã tạo thêm động lực để DNVVN phát triển các nguồn tài chính thay thế. Tại Latvia và Mexico, các sáng kiến Fintech đang được triển khai để hỗ trợ tài chính cho DNVVN trong bối cảnh khủng hoảng.

#### *Nâng cao năng lực quản lý và bảo vệ dữ liệu và quyền SHTT cho DNVVN*

DNVVN có xu hướng coi bí mật thương mại như là phương thức bảo vệ dữ liệu. Theo các kết quả khảo sát trước đây, các doanh nghiệp nhỏ coi bí mật thương mại là phương tiện quan trọng để bảo vệ đổi mới sáng tạo với lợi thế dẫn đầu về thời gian - đó là cơ chế chính của việc giành quyền SHTT trong một số ngành công nghiệp và thiết kế sản phẩm phức tạp - nhằm ngăn chặn đối thủ cạnh tranh làm hàng giả. Tuy nhiên, việc bảo hộ bí mật thương mại ngày càng khó khăn. Số hóa và cuộc cách mạng mã hóa, lưu trữ và trao đổi dữ liệu (nghĩa là ĐTĐM, email, ổ USB) là những yếu tố chính dẫn đến làm gia tăng các vụ vi phạm bí mật thương mại.

Bảo vệ dữ liệu cho DNVVN đang được tăng cường trong khi vẫn nỗ lực hài hòa hóa pháp luật giữa các khu vực tài phán và định hướng DNVVN thông qua các khung pháp lý khác nhau. Bí mật thương mại là chủ đề được chính sách trong nước và quốc tế chú ý nhiều và các luật về bí mật thương mại đã được tăng cường ở Châu Âu và Hoa Kỳ.

- Chỉ thị Bí mật thương mại châu Âu nhằm tiêu chuẩn hóa các luật quốc gia hiện hành và đa dạng chống lại việc thu thập, tiết lộ và sử dụng bất hợp pháp các bí mật thương mại. Chỉ thị có hiệu lực vào năm 2018, cho phép các doanh nghiệp khai thác và chia sẻ bí mật kinh doanh với các đối tác kinh doanh đặc quyền trên thị trường nội địa. Ví dụ, đăng ký bí mật thương mại trên blockchain có thể được coi là “bước hợp lý (...) để giữ bí mật [thông tin]”.

- Đạo luật Bảo vệ Bí mật thương mại của Hoa Kỳ năm 2016 nhằm tăng cường bảo vệ bí mật thương mại. Luật này đề cập đến quyền hành động dân sự liên bang và cung cấp lựa chọn giữa việc xử lý các tranh chấp tại địa phương theo luật tiểu

bang hoặc xử lý các tranh chấp theo luật liên bang. Tòa án có thể bảo vệ bí mật thương mại bằng cách ra lệnh chiếm đoạt, ra lệnh cho các bên đã chiếm đoạt bí mật thương mại tuân thủ các bước để giữ bí mật thương mại đó hoặc ra lệnh thanh toán tiền bản quyền, bồi thường thiệt hại, chi phí tòa án và phí thuê luật sư.

Liên minh châu Âu cũng đang tiến hành cải cách luật về quyền SHTT như một phần của gói biện pháp nhằm tạo lập thị trường kỹ thuật số. Cải cách bản quyền đặc biệt nhằm tăng khả năng tiếp cận xuyên biên giới với nội dung trực tuyến, mở ra nhiều cơ hội sử dụng tài liệu có bản quyền về giáo dục, nghiên cứu và di sản văn hóa và thị trường bản quyền hoạt động hiệu quả hơn. Bằng sáng chế Unitary sẽ cung cấp sự bảo hộ đồng nhất ở tối đa 26 quốc gia thành viên EU và mở ra cho các chủ sở hữu sáng chế một con đường thay thế cho các hệ thống sáng chế quốc gia và châu Âu hiện có, một thủ tục tại Văn phòng Sáng chế châu Âu (EPO) và một hệ thống kiện tụng thống nhất (Tòa án Sáng chế Thống nhất) sẵn sàng tăng khả năng đảm bảo về mặt pháp lý với chi phí giảm.

DNVVN được khuyến khích thu thập và quản lý kho dữ liệu ngày càng lớn trong bối cảnh tăng cường giám sát theo quy định, đặc biệt là bảo vệ dữ liệu và bí mật. Lo ngại về quyền riêng tư dữ liệu có thể làm gia tăng các rào cản mới đối với các doanh nghiệp nhỏ, ít năng lực để đối phó với môi trường pháp lý phức tạp. Quy định chung về bảo vệ dữ liệu (GDPR) do Liên minh châu Âu đưa ra vào tháng 5 năm 2018, nhằm hài hòa hóa luật bảo mật dữ liệu trên toàn châu Âu với mục tiêu rõ ràng là bảo vệ và trao quyền quyền riêng tư dữ liệu cho công dân EU và định hình lại cách các tổ chức tiếp cận vấn đề.

Ngoài ra, các nước đẩy mạnh sử dụng quyền SHTT giữa các DNVVN thông qua phổ biến thông tin, hỗ trợ tài chính và hỗ trợ kỹ thuật (Bảng 4).

Bảng 4. *Quản trị và bảo vệ dữ liệu trong DNVVN: Ví dụ từ các quốc gia*

Quốc gia	Sáng kiến	Mô tả
Áo	Sơ đồ sáng chế (Phiếu sáng chế)	Khoản tài trợ trị giá 12.500 EUR giúp các doanh nghiệp nhỏ đánh giá khả năng được cấp sáng chế cho các ý tưởng của họ với chuyên gia thẩm định sáng chế của văn phòng Sáng chế. Nếu được cấp sáng chế, khoản tài trợ sẽ bao gồm chi phí cho luật sư chuyên nghiệp tư vấn về sáng chế và phí đăng ký. Khoảng 80% người hưởng lợi cho đến nay là khách hàng mới sử dụng Hệ thống SHTT.
Đan Mạch	Cổng thông tin (Sáng kiến 2.2)	Một cổng thông tin sẽ được thành lập, cung cấp thông tin tư vấn, các công cụ cụ thể cho người dân, doanh nghiệp và cơ quan chức năng về bảo mật thông tin và

	(2018)	bảo vệ dữ liệu, cũng như thông tin về cách tuân thủ pháp luật hiện hành.
Hy Lạp	Miễn thuế sáng chế (Luật 3842/2010, điều 71)	Miễn thuế lợi nhuận từ việc bán các sản phẩm được bảo hộ bởi sáng chế được quốc tế công nhận, cho doanh nghiệp đã bán sản phẩm đó trong 3 năm tài chính liên tiếp sau khi đã đăng ký cho lần đầu bán. Các mục tiêu hướng đến là cung cấp các động lực mạnh mẽ cho doanh nghiệp thúc đẩy đầu tư NC&PT trong lĩnh vực kinh doanh và củng cố kết quả nghiên cứu và bảo vệ SHTT bằng cách có được các bằng sáng chế quốc tế và khai thác chúng.
Hàn Quốc	Dự án MyData	Hỗ trợ các dịch vụ cho phép các chủ thể dữ liệu tải trực tiếp dữ liệu cá nhân của họ do các tổ chức và doanh nghiệp sở hữu hoặc cung cấp dữ liệu đó với sự đồng ý của họ cho bên thứ ba sử dụng.
	Nền tảng dữ liệu lớn và Dự án mạng	Mục tiêu là hỗ trợ tạo ra dữ liệu và xây dựng cơ sở dữ liệu, hội tụ và phân tích dữ liệu cũng như phân phối và sử dụng dữ liệu thông qua hợp tác công-tư.
Tây Ban Nha	Kế hoạch chiến lược SHTT	Giới thiệu một số hành động nhằm nâng cao chất lượng, chuyển giao và quốc tế hóa SHTT. DNVVN được cấp các khoản tài trợ và trợ cấp để triển khai các mô hình sáng chế và tiện ích quốc gia. Các thỏa thuận giữa chính quyền các vùng và Văn phòng Nhãn hiệu và Sáng chế Tây Ban Nha cũng đã được ký kết để phát triển một mạng lưới các trung tâm trong vùng nhằm cung cấp cho người nộp đơn thông tin về quyền SHTT và vấn đề về khởi tố.

*Nguồn: Phản ứng của các quốc gia trong Khảo sát Tổng quan Kinh tế số của OECD về việc tiếp thu công nghệ số của doanh nghiệp năm 2019*

#### *Nâng cao khả năng bảo mật kỹ thuật số cho DNVVN*

DNVVN thường không có đủ nguồn lực hoặc chuyên môn để đánh giá hiệu quả rủi ro mạng và triển khai các biện pháp quản lý và phòng ngừa thích hợp. Siêu kết nối làm cho hạ tầng kỹ thuật số dễ bị tấn công. Các mối đe dọa bảo mật kỹ thuật số dường như đang ngày càng gia tăng về mức độ tinh vi, tần suất và cường độ, và các vi phạm không có chủ ý cũng có thể là do sử dụng sai dữ liệu cá nhân, ví dụ: do sự vô ý của nhân viên hoặc do vô tình làm mất dữ liệu. Mặc dù DNVVN là "mục tiêu nhỏ hơn" cho các cuộc tấn công mạng, nhưng nguy cơ xảy ra sự cố bảo mật sẽ tăng lên khi có sự ứng dụng rộng rãi của IoT, sự gia tăng của thương mại điện tử và sự nở rộ của dữ liệu lớn và việc sử dụng phân tích dữ liệu để khai

thác dữ liệu. Về điểm tích cực, DNVVN đảm bảo các hoạt động bảo mật và quyền riêng tư kỹ thuật số mạnh mẽ, sẽ có lợi thế cạnh tranh trong việc thiết lập quan hệ kinh doanh, đặc biệt là với các tập đoàn lớn. Do đó, khả năng của DNVVN đưa quản lý rủi ro bảo mật kỹ thuật số vào các giao thức hoạt động sẽ rất quan trọng để doanh nghiệp hội nhập vào nền kinh tế toàn cầu.

Các quốc gia đặc biệt chú trọng đẩy mạnh bảo mật kỹ thuật số giữa các DNVVN. Trong khảo sát năm 2017 của OECD, 82% quốc gia coi nhận thức về rủi ro bảo mật kỹ thuật số của DNVVN là một mục tiêu cụ thể. Tuy nhiên, chỉ 46% trong số đó đã triển khai các biện pháp khuyến khích cụ thể (thường và/hoặc biện pháp trừng phạt) để thúc đẩy quản lý rủi ro bảo mật kỹ thuật số. Nhật Bản và Hàn Quốc ưu đãi thuế cho các doanh nghiệp đầu tư vào các sản phẩm bảo mật kỹ thuật số.

Bảng 5. Chính sách bảo mật kỹ thuật số cho DNVVN: Ví dụ về quốc gia

Quốc gia	Sáng kiến	Mô tả
Cộng hòa Séc	Chiến lược An ninh mạng quốc gia (NCSS) (2015-2020)	Đây là tài liệu cơ bản của Chính phủ Séc về lĩnh vực an ninh mạng, phản ánh các lợi ích và nguyên tắc an ninh như được định nghĩa trong Chiến lược An ninh của Cộng hòa Séc.
	Đạo luật 181/2014 Coll., về An ninh mạng và thay đổi các đạo luật có liên quan (Đạo luật An ninh mạng)	Đạo luật này hệ thống hóa vai trò của Cơ quan An ninh mạng và Thông tin quốc gia (NĂŠKIB) và đặt nền tảng cho các quy định về an ninh mạng ở Cộng hòa Séc.
	Quy định (EU) 2019/881 về ENISA và chứng nhận an ninh mạng (Đạo luật an ninh mạng)	Đạo luật An ninh mạng đề cập đến việc ủy thác lâu dài cho ENISA (Cơ quan An ninh mạng của Liên minh châu Âu), tăng cường nguồn lực tài chính và nhân lực, cũng như nâng cao vai trò của ENISA trong việc hỗ trợ Liên minh châu Âu đảm bảo an ninh mạng ở mức phổ biến và ở cấp cao.
Đan Mạch	Công thông tin số chung dành cho báo cáo (sáng kiến 1.5) (2018-2019)	Mục đích là tạo ra các nền tảng chia sẻ thông tin liên quan đến vấn đề bảo mật.
	Chiến lược Bảo vệ mạng và thông tin Đan Mạch (2018-2023)	Mục đích là tạo ra tri thức và thúc đẩy hợp tác giữa người dân và doanh nghiệp về khía cạnh bảo mật khi ứng dụng các công nghệ số.
Estonia	Estonia khởi nghiệp	Sáng kiến này của chính phủ nhằm tăng cường hệ sinh thái khởi nghiệp địa phương, đặc biệt

	(2014)	là các vấn đề an ninh mạng
Singapore	Chứng nhận Số hóa DNVVN @ SGD (2014)	Cung cấp chứng nhận về chiến lược bảo mật kỹ thuật số cấp cao cho DNVVN.

*Nguồn: Phản ứng của các quốc gia trong Khảo sát Tổng quan Kinh tế số của OECD về việc tiếp thu công nghệ số của doanh nghiệp năm 2019.*

### *Thúc đẩy phát triển chính phủ điện tử và dịch vụ điện tử cho DNVVN*

Số hóa các dịch vụ công có thể mang lại một số lợi ích cho DNVVN. Số hóa giúp giảm bớt rắc rối do tình trạng quan liêu và chi phí giao dịch tương tác với cơ quan hành chính nhà nước, vốn có xu hướng chuyển một bộ phận tương đối lớn nguồn lực sang các chức năng hành chính. Số hóa dịch vụ công có thể làm tăng tính khả dụng dữ liệu về phương thức sử dụng và tùy chọn của người dùng cuối, cho phép triển khai cách tiếp cận lấy người dùng làm trung tâm trong việc phân bổ chính sách và tạo sân chơi bình đẳng cho các tương tác giữa chính phủ với DNVVN. Ngoài ra, số hóa dịch vụ công còn tạo động lực cho DNVVN tiếp tục áp dụng công nghệ. Theo khảo sát năm 2017 của các nước OECD, việc tăng cường các dịch vụ chính phủ điện tử, như xử lý trực tuyến các yêu cầu hành chính, là mục tiêu chính sách đầu tiên của các chiến lược số quốc gia và được coi là đòn bẩy chính để các cá nhân và doanh nghiệp ứng dụng CNTT nhiều hơn.

Các ứng dụng chính phủ điện tử đã phổ biến trên nhiều lĩnh vực, bao gồm dịch vụ phát triển kinh doanh, hệ thống li-xăng, kê khai thuế, đăng ký kinh doanh, hỗ trợ xuất khẩu, mua sắm công ...

Xu hướng ngày càng tăng liên kết giữa các cổng thông tin khác nhau để các doanh nghiệp không phải cung cấp thông tin giống nhau đáp ứng các nhu cầu khác nhau (nguyên tắc “chỉ một lần”). Thông thường, các cổng thông tin số đơn lẻ hoặc “một cửa” kỹ thuật số đóng vai trò là điểm đến duy nhất để truy cập các dịch vụ chính phủ điện tử và giảm bớt sự dư thừa các yêu cầu hành chính công. Các loại hình dịch vụ được cung cấp thông qua các nền tảng này, từ cung cấp thông tin và nâng cao nhận thức đến hỗ trợ thủ tục, cấp chứng nhận trực tuyến, mô phỏng và dự báo ...

Các yêu cầu giãn cách xã hội do đại dịch COVID-19 cũng đã nêu bật tầm quan trọng của việc sử dụng đầy đủ các nền tảng dịch vụ công của DNVVN để thông tin cho các doanh nghiệp và hỗ trợ của chính phủ cho các DNVVN và người kinh doanh tự do trong thời gian hoạt động kinh doanh tạm dừng.

*Bảng 6. Chính phủ điện tử và dịch vụ điện tử cho DNVVN: Ví dụ về quốc gia*

Quốc gia	Sáng kiến	Mô tả
----------	-----------	-------



Quốc gia	Sáng kiến	Mô tả
Một cửa, cổng thông tin số và các ứng dụng hướng đến các dịch vụ công		
Áo	Giảm phí liên bang cho các dịch vụ công (2016)	Ưu đãi tài chính (giảm 40% chi phí) khi sử dụng các ứng dụng trực tuyến. Chương trình này không tập trung vào DNVVN.
Cộng hòa Séc	Cổng dịch vụ công (2016)	Dự án này sẽ giảm bớt gánh nặng hành chính, điện tử hóa các quy trình nội bộ của hành chính công và đưa hành chính công đến gần hơn với khách hàng.
Latvia	Hệ thống ứng dụng điện tử (2007)	Cung cấp cho người dùng tiện ích gửi tài liệu và nhập tất cả dữ liệu để theo dõi thông tin thực tế và dòng tài chính cá nhân. Hơn 30 dịch vụ có sẵn trong Hệ thống ứng dụng điện tử, sẽ tránh tình trạng khách hàng phải đứng xếp hàng và nộp tài liệu bản giấy tại các trung tâm khách hàng.
Thổ Nhĩ Kỳ	Hệ thống Chính phủ điện tử KOSGEB	Theo Nghị định thư được ký kết với 12 tổ chức chính phủ của Thổ Nhĩ Kỳ, Tổ chức Phát triển DNVVN (KOSGEB) có thể truy cập trực tuyến dữ liệu tài chính và thống kê của DNVVN. Từ năm 2018, tất cả các ứng dụng và quy trình liên quan đến các chương trình hỗ trợ DNVVN của KOSGEB có thể được thực hiện thông qua hệ thống chính phủ điện tử KOSGEB. Vào tháng 9/2020, 23 dịch vụ số đã được cung cấp theo cách này.
Lập hóa đơn điện tử, chữ ký điện tử và tuân thủ thuế		
Úc	Bảng lương một lần chạm (Single touch payroll) (từ 2018)	Cung cấp quy trình xử lý tự động, hợp lý hóa các nghĩa vụ liên quan đến người sử dụng lao động cùng với thời điểm trả lương theo định kỳ. Thông qua cho phép báo cáo theo thời gian thực, chính sách này mở ra cơ hội tăng cường chia sẻ giữa các cơ quan chính phủ.
Áo	Quy định về hóa đơn điện tử (từ 2014)	Từ năm 2014, các đối tác theo hợp đồng của chính phủ liên bang trong các giao dịch hàng hóa và dịch vụ có nghĩa vụ chỉ gửi hóa đơn ở dạng điện tử.
Chile	Sửa đổi Đạo luật Chữ ký điện tử (2019)	Mục tiêu của sáng kiến là tăng cường khả năng tiếp nhận và sử dụng chữ ký điện tử.
Colombia	Ban hành nghị định quy định về sự tương tác của hồ sơ y tế điện tử,	Chính sách này đưa ra định nghĩa về các tiêu chuẩn tương tác để truyền tải thông tin, định nghĩa về mô hình hoạt động và mô hình trưởng thành (maturity

Quốc gia	Sáng kiến	Mô tả
	điều 246 của luật 1955 năm 2019 (2019)	model).
Cộng hòa Séc	Công thông tin Thuế hiện đại và dễ truy cập (2018-2025)	Quản lý thuế đơn giản và tiện lợi tại một điểm.
	Truyền dữ liệu từ các báo cáo tài chính (2018-2022)	Cơ quan quản lý thuế sẽ đảm bảo việc chuyển dữ liệu đã chọn lọc từ các báo cáo tài chính đến các cơ quan đăng ký để xuất bản dữ liệu trong Bộ sưu tập tài liệu. Điều này chỉ được áp dụng cho dữ liệu được nộp cho cơ quan thuế dưới dạng điện tử.
	Khai thuế điện tử (từ 2020)	Cho hoãn khai thuế điện tử một tháng.
Na Uy	Quy định Lập hóa đơn điện tử (2019)	Sáng kiến đưa ra quy định bắt buộc các cơ quan trong khu vực công phải xuất hóa đơn điện tử ở định dạng tiêu chuẩn có thể đọc được bằng máy khi mua sắm hàng hóa và dịch vụ từ khu vực tư nhân.
Dữ liệu mở của chính phủ		
Colombia	Tăng cường thông tin y tế và hệ thống bảo trợ xã hội quốc gia (2019-2022)	Hệ thống thông tin y tế và bảo trợ xã hội sẽ được tăng cường thông qua kết nối các hệ thống thông tin và công cụ công nghệ và áp dụng các biện pháp để tạo điều kiện sử dụng dữ liệu.
Cộng hòa Séc	Đạo luật Sức khỏe điện tử và Chia sẻ dữ liệu đảm bảo giữa các nhà cung cấp dịch vụ chăm sóc sức khỏe (2020)	Chính sách tập trung vào sức khỏe điện tử và đơn giản hóa hợp tác giữa các nhà cung cấp dịch vụ chăm sóc sức khỏe. Bản thân nhà cung cấp là một công cụ quản lý.
Latvia	Hệ thống Thông tin kiểm soát và nghề cá tổng hợp	Cung cấp cơ sở dữ liệu CNTT cho ngành công nghiệp nghề cá.

*Nguồn: Phản ứng của các quốc gia trong Khảo sát Tổng quan Kinh tế số của OECD về việc tiếp thu công nghệ số của doanh nghiệp.*

*Triển khai cơ sở hạ tầng và nền tảng số chất lượng cao*

Hạ tầng CNTT&TT rất quan trọng để duy trì khả năng phổ biến kỹ thuật số giữa các DNVVN. Các nghiên cứu về doanh nghiệp Đức và Ai-len đã chỉ ra rằng việc sử dụng kết nối băng thông rộng tác động lớn và tích cực đến hoạt động đổi mới sáng tạo của doanh nghiệp. Truy cập mạng tốc độ cao cho phép DNVVN kết nối với nhà cung cấp và khách hàng, thu thập thông tin thời gian thực và đưa ra phản ứng theo thời gian thực cho các thị trường và chuỗi cung ứng đang phát triển nhanh. Mạng kỹ thuật số tốc độ cao cũng cho phép các doanh nghiệp nhỏ xây dựng năng lực kỹ thuật số, ví dụ, thông qua các dịch vụ ĐTĐM. Mặc dù các doanh nghiệp đang ngày càng hướng đến dùng băng thông rộng cố định tốc độ cao do phí truy cập phải chăng và triển vọng thị trường của nền kinh tế ứng dụng sôi động, nhưng khoảng cách giữa các quốc gia và các doanh nghiệp ngày càng nới rộng, trong đó, các doanh nghiệp nhỏ đang mất dần vị thế trong quá trình chuyển đổi.

Các doanh nghiệp hướng nhiều đến công cụ đám mây để truy cập email, dung lượng lưu trữ hoặc quản lý dữ liệu. ĐTĐM cho phép DNVVN truy cập thêm dung lượng xử lý hoặc lưu trữ, cũng như cơ sở dữ liệu và phần mềm, với số lượng phù hợp và theo nhu cầu. Ngoài tính linh hoạt và khả năng mở rộng, ĐTĐM còn giảm chi phí nâng cấp công nghệ thông qua miễn các khoản đầu tư trả trước cho phần cứng và chi phí thường xuyên cho bảo trì, đội ngũ CNTT và việc chứng nhận. Ngoài ra, ĐTĐM còn giúp phổ biến các công nghệ khác và cho phép bắt kịp công nghệ. Các hình thức làm việc di động mới đã góp phần làm tăng tính phổ biến của ĐTĐM khi các doanh nghiệp có thể áp dụng các công nghệ độc lập với nền tảng truy cập được ở mọi nơi và từ bất kỳ thiết bị nào (như điện thoại thông minh, máy tính để bàn, máy tính xách tay...). Trong tương lai gần, DNVVN có thể mở rộng sử dụng dịch vụ ĐTĐM vì các chủ DNVVN nhận thức được tiềm năng của ĐTĐM làm tăng tính linh hoạt và giảm chi phí.

Tuy nhiên, vấn đề lòng tin vẫn là trở ngại lớn. Rõ ràng việc duy trì quyền sở hữu dữ liệu là lý do chính để DNVVN không từ bỏ các giải pháp dữ liệu và CNTT tại chỗ. Việc mất quyền kiểm soát dữ liệu thực sự có liên quan mật thiết đến tính không ổn định của vị trí dữ liệu, làm gia tăng bất ổn xoay quanh quy định bảo vệ dữ liệu được áp dụng và các khu vực pháp lý mà quy định đó được thực thi.

Tương tự như vậy, việc thiếu các tiêu chuẩn mở trong cộng đồng các nhà cung cấp dịch vụ đám mây làm tăng khó khăn cho người dùng ĐTĐM khi chuyển đổi giữa các nhà cung cấp và nguy cơ bị mắc kẹt công nghệ (technological lock-in). Do đó, người dùng có thể rất dễ bị ảnh hưởng bởi chính sách giá của nhà cung cấp, đặc biệt là khi sự phát triển mới trong phân tích dữ liệu sẽ cho phép họ lập hồ sơ người dùng và phân biệt giá cả. Lo ngại càng gia tăng do sự tập trung thị trường ở mức cao hiện nay của ngành công nghiệp đám mây.

Nhiều quốc gia đã thực hiện chiến lược toàn diện với trọng tâm nhằm tăng cường đối thoại công-tư và sự tham gia phát triển hạ tầng của khu vực tư nhân. Ngoài ra, các chính quyền địa phương đóng vai trò quan trọng trong bối cảnh cơ sở hạ tầng và các chính sách hạ tầng khu vực và thành phố có khả năng phát triển phù hợp, vì các thành phố và khu vực ngày càng có trách nhiệm thiết kế và thực hiện chính sách trong các lĩnh vực quan trọng đối với DNVVN như băng thông rộng. Trong một không gian rộng lớn và phức tạp như vậy, phương pháp tiếp cận toàn chính phủ (gồm có các bộ, ban, ngành ở các cấp thẩm quyền) trở nên cần thiết, có đề cập đến các tác động có liên quan và những lợi ích đan xen và đa dạng. Chính phủ các nước cũng áp dụng các hình thức quản trị kết hợp có sự tham gia ngày càng nhiều của các doanh nghiệp nhỏ vào các cuộc tranh luận chính sách và quá trình hoạch định chính sách, ví dụ: thông qua tham vấn cộng đồng hoặc cơ chế thảo luận nhiều bên liên quan.

Các nước cũng đang khuyến khích DNVVN tiếp cận cơ sở hạ tầng và nền tảng mạng quan trọng, thông qua việc thiết lập và chia sẻ các nền tảng cung cấp môi trường trao đổi kiến thức và chuyên môn, đồng thời góp phần vào việc kết nối mạng lưới, phổ biến thông tin và cộng tác. Các nền tảng và hoạt động của các cụm cho phép DNVVN tiếp cận với các công nghệ mà họ không có khả năng tự mua. Hơn nữa, DNVVN hoạt động trong các cụm có thể được hưởng lợi từ các hiệu ứng kết tụ khác, chẳng hạn như cải thiện khả năng tiếp cận nguồn lao động lành nghề hoặc khả năng được các nhà đầu tư mạo hiểm biết đến.

Việc sử dụng chung thiết bị nghiên cứu để khai thác thiết bị tiên tiến hoặc quyền truy cập vào khả năng tính toán của siêu máy tính nhằm mục đích tận dụng tiềm năng của dữ liệu lớn là những ví dụ về các lựa chọn chính sách được áp dụng.

*Bảng 7. Chính sách hạ tầng, nền tảng và phương tiện mạng: Ví dụ từ các quốc gia*

Quốc gia	Sáng kiến	Mô tả
<b>Kế hoạch hạ tầng số</b>		
Úc	Nhà vô địch kỹ thuật số là doanh nghiệp nhỏ (2019-2021)	Với ngân sách 8,9 triệu AUD, chương trình nhằm đẩy mạnh tương tác giữa các doanh nghiệp số nhỏ và các nhà lãnh đạo hoặc nhà đổi mới nổi tiếng ở Úc thông qua tài trợ trực tiếp và dịch vụ theo dõi (tư vấn).
Áo	Lộ trình kỹ thuật số của Áo (2016) và nước Áo kỹ thuật số (2018)	Mục đích của chương trình là kết nối những người tiên phong trong lĩnh vực kỹ thuật số với các doanh nghiệp đã thành lập để nâng cao kiến thức.
Costa Rica	Nền kinh tế số trụ cột (2019-2021)	Chương trình đảm bảo khả năng tiếp cận các dịch vụ viễn thông, phổ vô tuyến sẵn có, triển khai cơ

Quốc gia	Sáng kiến	Mô tả
		sở hạ tầng bền vững theo cách có trật tự, cũng như các quy tắc thị trường rõ ràng.
Ai-len	Kế hoạch viễn thông (2019-2033)	Kế hoạch nhằm kết nối 99,9% hộ gia đình và doanh nghiệp của Ai-len với cáp quang. Ngoài ra, kế hoạch còn kết nối quốc tế thông qua ba cáp ngầm ở các vị trí khác nhau. Việc triển khai 5G cũng là một mục tiêu của chính sách này. Ai-len muốn giữ vai trò dẫn đầu trong việc sử dụng 5G. Kết nối di động phải được đảm bảo, ví dụ: ở các thành phố và thị trấn, trên đường cao tốc, các địa điểm du lịch nổi tiếng và dọc theo đường bờ biển của đất nước.
Latvia	Chương trình Phát triển Nông thôn Latvia (2014-2020)	Nhằm mục đích tăng năng lực cạnh tranh của nông dân Latvia và các doanh nghiệp nông thôn bằng cách cải thiện cơ sở hạ tầng và cung cấp các dịch vụ tư vấn và đào tạo.
	Đầu tư tài sản vật chất (như một phần chương trình Phát triển Nông thôn của Latvia 2014-2020)	Hỗ trợ hiện đại hóa và phát triển các cơ sở nông nghiệp, bao gồm cả việc áp dụng các công nghệ chính xác trong các trang trại. Nông nghiệp chính xác là một phương pháp quản lý toàn trang trại thông qua sử dụng công nghệ thông tin, dữ liệu định vị vệ tinh (GNSS), viễn thám và thu thập dữ liệu gần.
Thổ Nhĩ Kỳ	Cơ quan công nghệ Thông tin và Truyền thông (2019-2023)	Mục tiêu chính là chuẩn bị hệ sinh thái quốc gia (cả công và tư) cho sự phát triển vượt bậc của công nghệ 5G.
Nền tảng và giao diện kết nối mạng với khu vực doanh nghiệp		
Bỉ	Cluster software.brussel	Nền tảng dành cho các bên liên quan của ngành công nghiệp phần mềm tại Brussels, cung cấp dịch vụ hỗ trợ cá nhân và nhóm làm việc, dịch vụ mạng và nâng cao kỹ năng.
Đức	Sáng kiến Trung tâm kỹ thuật số (2017)	Chương trình nhằm tăng cường kết nối và hợp tác giữa các công ty khởi nghiệp, DNVVN, nhà khoa học và nhà đầu tư tại 12 trung tâm xuất sắc và tăng khả năng hiện diện của họ ở nước ngoài.
	Trung tâm Năng lực Kỹ thuật số DNVVN (2015-2022)	Hỗ trợ DNVVN số hóa, kết nối mạng và giới thiệu các ứng dụng của Công nghiệp 4.0.
	Mạng lưới có cấu trúc	Sáng kiến được tài trợ công nhằm hỗ trợ hoạt

Quốc gia	Sáng kiến	Mô tả
Hy Lạp	hỗ trợ doanh nghiệp (2014-2020)	động khởi nghiệp trong nước. Mục tiêu tổng thể là tăng cường chuyển đổi số
	Tham gia mạng lưới doanh nghiệp châu Âu (2016)	Đây là liên minh chiến lược của các mạng lưới hỗ trợ doanh nghiệp lớn (trung tâm nghiên cứu và công nghệ, liên đoàn công nghiệp, phòng thương mại và cơ quan phát triển) ở Hy Lạp. Mạng lưới cung cấp các dịch vụ hỗ trợ tinh thần khởi nghiệp, đổi mới sáng tạo và DNVVN.
	Trung tâm trí tuệ nhân tạo (AI) xuất sắc (2019-2024)	Chương trình nhằm mục đích thành lập một Trung tâm xuất sắc, nơi sẽ kết nối các nhà nghiên cứu, nhà khoa học và chuyên gia AI với các nhân viên kinh doanh từ nhiều lĩnh vực công nghiệp và sử dụng các công nghệ mới để tăng tốc đổi mới.
	Orange grove Athens (2013)	Một cộng đồng mạng và không gian làm việc chung linh hoạt dành cho các doanh nhân trẻ ở Hy Lạp.
Ý	Đoàn kết kỹ thuật số	Sáng kiến này do Bộ Đổi mới và Số hóa phát động trong bối cảnh COVID-19, bao gồm một cổng thông tin nơi các doanh nghiệp (cụ thể là DNVVN) có thể đăng ký truy cập mà không phải trả phí dịch vụ kỹ thuật số cho các doanh nghiệp lớn trong khu vực tư nhân liên quan đến làm việc thông minh/từ xa, hội nghị truyền hình, truy cập dữ liệu di động, ĐTĐM ... để ứng phó với những hạn chế trong di chuyển và làm việc.
Slovenia	Trung tâm đổi mới kỹ thuật số Slovenia (2019-2023)	Sáng kiến này cung cấp, kết nối và hỗ trợ kiến thức, chuyên môn kinh doanh, công nghệ và trao đổi các phương pháp hay nhằm hỗ trợ đầy đủ cho ngành công nghiệp Slovenia trong việc xây dựng năng lực kỹ thuật số, các mô hình và quy trình đổi mới, hỗ trợ chuyển đổi số và tăng lợi thế cạnh tranh của doanh nghiệp.

## II. TĂNG CƯỜNG BẢO MẬT KỸ THUẬT SỐ CHO DOANH NGHIỆP VỪA VÀ NHỎ

### 2.1. Thách thức trong việc tăng cường bảo mật kỹ thuật số

*Bản chất và diễn biến của rủi ro bảo mật kỹ thuật số*

Sự cố trong bảo mật kỹ thuật số gây thiệt hại cho các doanh nghiệp, chính phủ và cá nhân thông qua làm suy yếu tính khả dụng, tính toàn vẹn và/hoặc tính bảo mật của các hệ thống và mạng lưới dữ liệu, thông tin. Rò rỉ dữ liệu là một trong những sự cố ảnh hưởng đến tính bảo mật của dữ liệu dẫn đến việc tiết lộ dữ liệu cho bên không được phép biết. Do hậu quả của các sự cố bảo mật kỹ thuật số, nạn nhân có thể phải đối mặt với những thiệt hại hữu hình và vô hình như tổn thất tiền bạc, giảm khả năng cạnh tranh, giảm danh tiếng, gián đoạn hoạt động, vi phạm quyền riêng tư ...

Rủi ro bảo mật kỹ thuật số là kết quả của các sự cố do các mối đe dọa từ việc khai thác lỗ hổng bảo mật gây ra. Các nguồn đe dọa bao gồm các chính phủ, nhóm và cá nhân có ý đồ xấu và/hoặc mục đích phạm tội. Động cơ tấn công rất khác nhau, với các chính phủ là nhằm mục tiêu địa chính trị, với tội phạm là kiếm tiền, với kẻ khủng bố là bạo lực, chỉ đơn thuần là mục đích cá nhân đối với những người thích tìm cảm giác mạnh và sự bất bình đối với các mối đe dọa nội bộ.

Các sự cố cũng có thể bắt nguồn từ các yếu tố ngoài ý muốn như lỗi của con người, lỗi hệ thống hoặc các nguyên nhân khách quan bên ngoài (như mất điện, sét đánh, pháo sáng mặt trời). Các sự cố này có thể do một tác nhân độc hại bên ngoài thông qua sử dụng các phương pháp kỹ thuật xã hội như lừa đảo. Tuy nhiên, do cách thức thiết kế các hệ thống và phần mềm kỹ thuật số, người dùng công nghệ có thể phạm sai lầm và gây ra tổn thất tài chính.

#### *Các cuộc tấn công mạng thường liên quan đến lỗi của con người*

Việc đo lường mức độ phổ biến và chi phí của các sự cố kỹ thuật số vẫn là thách thức do thiếu các tiêu chuẩn quốc tế và dữ liệu có thể so sánh. Các doanh nghiệp hoặc là không hiểu mức độ rủi ro thực sự; hoặc không phát hiện ra sự cố; hoặc không đo lường tác động của chúng theo cách tiêu chuẩn; và không báo cáo. Tuy nhiên, khi được diễn giải thận trọng, có thể thấy một số xu hướng nảy sinh.

Verizon, một doanh nghiệp viễn thông lớn của Hoa Kỳ, gần đây đã công bố Báo cáo Sự cố rò rỉ dữ liệu năm 2020. Dữ liệu được thu thập từ các đại diện của chính phủ và phi chính phủ tại 81 quốc gia. Kết quả cho thấy 70% sự cố rò rỉ là do các tác nhân bên ngoài. 55% trong số đó là do các nhóm tội phạm có tổ chức thực hiện. Tuy nhiên, lỗi cũng rất phổ biến, gây ra 22% số vụ rò rỉ, phổ biến hơn phần mềm độc hại, tức là mã độc. Ví dụ, lỗ hổng bảo mật phát sinh khi quản trị viên hệ thống lơ là trong việc áp dụng các biện pháp kiểm soát bảo mật để hạn chế quyền truy cập vào dữ liệu của doanh nghiệp được đăng trên nền tảng đám mây (lỗi cấu hình) hoặc mối đe dọa tăng lên khi dữ liệu nhạy cảm được chuyển đến sai người nhận. Trong các trường hợp khác, có thể là lỗi gửi thư hàng loạt khi các địa chỉ không còn được ghép nối với nội dung chính xác. Những lỗi này, bao gồm quản trị

không đúng, vô tình làm lộ máy chủ hoặc cấu hình sai các giao thức và điều khiển, có thể liên quan đến việc chuyển đổi nhanh sang công cụ đám mây và thiếu hiểu biết chung về bảo mật môi trường và dịch vụ đám mây.

### *Các mối đe dọa ngày càng tinh vi, khó phát hiện và xử lý*

Một số phương thức tấn công mạng có mục tiêu và tinh vi hơn theo thời gian, khiến các doanh nghiệp, tổ chức và chính phủ khó phát hiện và xử lý. Các cuộc tấn công, kỹ thuật và phương thức tiếp cận độc hại phát triển liên tục để trốn tránh cơ quan thực thi pháp luật, cản trở nỗ lực bảo vệ và ngăn ngừa bảo mật kỹ thuật số, cũng như thích ứng tốt hơn với các lỗ hổng mục tiêu.

Tuy nhiên, những kẻ tấn công trước tiên đều thử các phương pháp tấn công cũ và rẻ tiền, và chỉ tăng độ tinh vi khi thu được lợi ích tương xứng. Nhiều doanh nghiệp, đặc biệt là những doanh nghiệp nhỏ, bị dính các cuộc tấn công đơn giản do thiếu sự bảo vệ cơ bản và phương thức tăng cường bảo mật kỹ thuật số tối thiểu. Các phương pháp tinh xảo hơn có xu hướng nhằm vào các doanh nghiệp được bảo mật kỹ thuật số tốt hơn. Các cuộc tấn công lừa đảo, từ chối dịch vụ và phần mềm mã độc tiếp tục phổ biến trong bối cảnh kỹ thuật số.

### *Hầu hết các sản phẩm chứa mã phần mềm, đều có lỗ hổng bảo mật*

Các cuộc tấn công nổi tiếng như dùng phần mềm mã độc WannaCry và NotPetya, đã cho thấy những lỗ hổng lớn về bảo mật kỹ thuật số trong hàng nghìn doanh nghiệp và tổ chức thuộc khu vực công, đặc biệt liên quan đến giai đoạn cuối của các sản phẩm có chứa mã phần mềm. Theo ước tính, có từ 20 đến 100 lỗ hổng trong mỗi dòng của 2.000 dòng mã. Diễn giải theo cách dễ hiểu, thì một ứng dụng iPhone trung bình có khoảng 50.000 dòng mã, trong khi Android có khoảng 12 triệu dòng mã và Windows 10 có hơn 50 triệu dòng mã. Trung bình, 46 lỗ hổng mới được phát hiện và tiết lộ công khai mỗi ngày, bao gồm cả các sản phẩm được sử dụng rộng rãi như Android, iOS hoặc Windows.

Các sản phẩm ngày càng ứng dụng nhiều kỹ thuật số và toàn bộ các lĩnh vực đều phụ thuộc vào kỹ thuật số. Về phía người tiêu dùng, hàng hóa truyền thống đang trở nên “thông minh”, tức là chứa mã và kết nối với nhau (ví dụ, ô tô và thiết bị gia dụng được kết nối). Số lượng thiết bị kết nối ước tính lên đến 20 tỷ trên toàn cầu vào năm 2020. Về phía doanh nghiệp, họ sử dụng ngày càng nhiều phần mềm để thực hiện các chức năng cốt lõi như sản xuất và phân phối, cũng như phát triển ĐTĐM và các mô hình đăng ký phần mềm cho các hoạt động thường xuyên.

### *Mức độ phổ biến và chi phí của các sự cố bảo mật kỹ thuật số*

Ngày nay, các tổ chức ở mọi quy mô đều gặp rắc rối với các cuộc tấn công vào các ứng dụng web, thiết bị người dùng, máy chủ và con người (các cuộc tấn



công nghệ thuật xã hội). Ở châu Âu, tỷ lệ các doanh nghiệp gặp sự cố bảo mật CNTT&TT trong năm 2019, chẳng hạn như không có sẵn các dịch vụ CNTT&TT, phá hủy hoặc hỏng dữ liệu hoặc tiết lộ dữ liệu bí mật, trung bình là 13%, nhưng dao động từ 6% (Vương quốc Anh) đến 35% (Thụy Điển). Dữ liệu của OECD bổ sung cho bức tranh cho các quốc gia không thuộc EU và cho thấy từ 10% đến 20% doanh nghiệp (có từ 10 người) đã gặp sự cố vi phạm bảo mật trong năm 2019, điển hình như Nhật Bản (56%), trong khi Hàn Quốc chỉ 5%. 30% doanh nghiệp Ý đã báo cáo ít nhất đã chịu một số thiệt hại từ tấn công mạng trong giai đoạn từ tháng 9 năm 2015 đến tháng 9 năm 2016.

*Mục tiêu lý tưởng: Các tổ chức có dữ liệu giá trị dễ bị tấn công*

Dữ liệu mà một doanh nghiệp sở hữu, cũng như khả năng tài chính và tiền bạc (tức là số tiền mà doanh nghiệp sở hữu hoặc xử lý), là những động cơ chính đằng sau phần lớn các cuộc tấn công bảo mật kỹ thuật số. Mặc dù một nhóm nhỏ các cuộc tấn công được thực hiện với mục đích gián điệp, nhưng phần lớn những kẻ đe dọa nhằm tìm cách đột nhập và đánh cắp thứ gì đó có giá trị để bán (dữ liệu, bí mật thương mại, tài sản trí tuệ...) hoặc rửa tiền.

Tội phạm thông thường chủ yếu quan tâm đến việc lấy thông tin xác thực và dữ liệu cá nhân. Sau hai mục tiêu đó, dữ liệu y tế, nội bộ hoặc thanh toán có mức độ quan tâm gần như nhau. Lừa đảo qua gửi email hàng loạt vẫn là phương tiện dễ dàng, ít tốn kém và hiệu quả nhất, bao gồm cả việc đánh cắp thông tin đăng nhập, sau đó dùng giao dịch trên trang web đen mà chủ nhân của chúng thậm chí không hề hay biết. Rủi ro và lợi nhuận liên quan đến thông tin đăng nhập bị đánh cắp, có thể ở mức cao khi các cá nhân sử dụng lại thông tin đăng nhập của họ cho nhiều tài khoản và các tổ chức không triển khai các phương pháp xác thực đa yếu tố.

Toàn cầu hóa cũng có thể vừa là kênh chống lại rủi ro bảo mật kỹ thuật số bổ sung, vừa là kênh học hỏi kinh nghiệm và quản lý rủi ro tốt hơn. Vì “các doanh nghiệp tầm cỡ quốc tế có nhiều kinh nghiệm kinh doanh trực tuyến, dẫn đến nhận thức tốt hơn mối đe dọa cao và họ dễ bị tấn công xuyên biên giới hơn (Biancotti, 2017 [19]).”

*DNVVN có ít điểm dễ tấn công hơn nhưng có thể phải chịu chi phí tương đối cao do sự cố bảo mật*

Tính trung bình, DNVVN có cường độ số hóa thấp hơn và một danh mục tài sản kỹ thuật số nhỏ hơn cần được quản lý và bảo vệ. Tuy nhiên, điều đó không có nghĩa là họ không phải chịu rủi ro về bảo mật kỹ thuật số. DNVVN với tư cách là người dùng và đôi khi là nhà sản xuất công nghệ kỹ thuật số, phải chịu rủi ro, đó là các lỗ hổng trong các công nghệ này có thể bị các đối tượng xấu khai thác. Trước đây, DNVVN ít có khả năng phát hiện và báo cáo các vi phạm bảo mật kỹ thuật số

hơn các doanh nghiệp lớn. Điều này do nhiều nguyên nhân bao gồm: ít nhân lực nên dễ xảy ra sai sót; kỹ năng và nhận thức nội bộ hạn chế trong việc phát hiện và giải quyết các sự cố; và ít tiếp cận với nguồn tài chính để đầu tư vào khả năng bảo vệ và/hoặc phát hiện.

#### *Thiệt hại lên đến hàng tỷ USD với các chi phí ngầm*

Khi sự cố kỹ thuật số xảy ra do vô tình hay cố ý, doanh nghiệp không thể hoạt động bình thường và phải chịu thêm chi phí và tổn thất, tùy thuộc vào bản chất của sự cố (như chi phí pháp y, chi phí gián đoạn kinh doanh, chi phí pháp lý, tiền phạt theo quy định...). Điều quan trọng là phải phân biệt giữa chi phí, tổn thất và chi phí cơ hội, vì các yếu tố này thường không được phân biệt rõ trong các tài liệu kinh tế về bảo mật kỹ thuật số.

Các ước tính về tổn thất do sự cố bảo mật kỹ thuật số rất hiếm và thường bị đánh giá thấp. Một cách để tính toán tổn thất là xem xét các yêu cầu bảo hiểm. Các hợp đồng bảo hiểm nhằm bù đắp những tổn thất do một số loại sự cố bảo mật kỹ thuật số gây ra. Khi doanh nghiệp yêu cầu bồi thường theo các chính sách này và dữ liệu khiếu nại được công khai, có thể thấy số tiền thực tế bị mất. Tuy nhiên, số tiền này có thể thấp hơn tổng thiệt hại kinh tế. Các chi phí và tổn thất phát sinh do sự cố bảo mật kỹ thuật số cũng tăng lên theo quy mô doanh nghiệp.

#### *Quá trình chuyển đổi kỹ thuật số và rủi ro bảo mật gia tăng*

*Chuyển đổi số làm tăng khả năng doanh nghiệp tiếp cận với rủi ro bảo mật kỹ thuật số*

Các công nghệ số mới có tiềm năng thúc đẩy đổi mới, nâng cao năng suất và cải thiện hạnh phúc. Nhiều DN VN được hưởng lợi từ các sản phẩm và phương thức kỹ thuật số mới, tạo cơ hội để họ vượt qua các rào cản về quy mô thường gặp trong quá trình đổi mới, vươn ra toàn cầu và phát triển.

Tuy nhiên, chuyển đổi số cũng làm tăng sự phụ thuộc của doanh nghiệp vào kỹ thuật số và tăng rủi ro bảo mật kỹ thuật số. Sự tiến bộ của công nghệ máy tính và khả năng lưu trữ đã khuyến khích việc sử dụng rộng rãi các thiết bị máy tính cá nhân và tạo ra dữ liệu. Internet, ứng dụng thông minh và dữ liệu lớn làm tăng khối lượng dữ liệu có sẵn. Băng thông rộng 5G làm tăng tốc độ và khối lượng truyền dữ liệu. AI thúc đẩy sử dụng dữ liệu. Ngoài ra, rủi ro không đáng kể là AI tạo ra những thách thức mới về bảo mật kỹ thuật số.

Trên thực tế, sự cố bảo mật kỹ thuật số có thể ảnh hưởng đến tất cả các hệ thống thông tin, bao gồm cả những hệ thống dựa vào AI, IoT, tức là siêu kết nối của các cảm biến, thiết bị và hệ thống hỗ trợ giao tiếp giữa máy với máy, sẽ làm tăng mạnh khối lượng dữ liệu có sẵn (và có thể khai thác thông qua AI và máy

học). Tuy nhiên, với IoT, khả năng xảy ra sự cố bảo mật có thể cao hơn, các thành phần IoT vừa trở thành mục tiêu của các cuộc tấn công, vừa là kênh để phá vỡ các hệ thống vật lý. Vì IoT kết nối thế giới trực tuyến và ngoại tuyến, nên các thiệt hại kỹ thuật số có thể mở rộng sang môi trường vật lý. Các cuộc tấn công mạng làm thay đổi hoạt động của các hệ thống điều khiển và giám sát (như ô tô tự lái, thiết bị y tế...) hoặc các hệ thống quốc phòng và an ninh và làm gián đoạn việc cung cấp các dịch vụ thiết yếu (như điện, nước, sưởi ấm, tài chính, giao thông) với hậu quả gây chết người.

ĐTĐM cho phép tiếp cận thêm khả năng xử lý hoặc dung lượng lưu trữ trực tuyến, cũng như cơ sở dữ liệu và phần mềm, đồng thời hỗ trợ phổ biến các công nghệ số khác, cũng như các phương thức kinh doanh sáng tạo. Do tính linh hoạt và khả năng mở rộng, ĐTĐM giảm chi phí nâng cấp công nghệ bằng cách miễn các khoản đầu tư trả trước cho phần cứng và chi phí thường xuyên cho việc bảo trì, đội ngũ CNTT và việc chứng nhận, biến mô hình quản lý CNTT&TT thành mô hình dựa trên việc mua lại phần mềm (mã) và (siêu) kết nối kỹ thuật số.

Dữ liệu ứng dụng CNTT trong doanh nghiệp tại các nước OECD và EU nêu bật mối quan hệ chặt chẽ giữa lỗ hổng kỹ thuật số, siêu kết nối và mã hóa. Khi các doanh nghiệp có xu hướng mua nhiều các dịch vụ ĐTĐM hoặc người lao động sử dụng máy tính có kết nối Internet, thì doanh nghiệp nhiều khả năng gặp các sự cố bảo mật liên quan đến CNTT&TT. Trên thực tế, kết nối ngày càng tăng của các hoạt động sử dụng nhiều dữ liệu làm tăng tính phức tạp, biến động và phụ thuộc vào các cơ sở hạ tầng và quy trình hiện có.

*Số hóa làm tăng giá trị kinh tế của dữ liệu và thúc đẩy việc đánh cắp dữ liệu khi các DN VN không được chuẩn bị tốt phương tiện bảo vệ*

Dữ liệu chưa bao giờ phổ biến như hiện nay và số hóa đã biến dữ liệu thành tài sản chiến lược. Dữ liệu được tạo ra ngày càng nhiều cùng với các hoạt động kinh doanh, ví dụ: sản xuất và cung cấp (dữ liệu xử lý) và được tổng hợp ở các giai đoạn khác nhau của giao dịch kinh doanh (dữ liệu người dùng, người tiêu dùng và nhà cung cấp). Dữ liệu xử lý có thể cải thiện công tác quản lý kho, logistics và bảo trì, cũng như khả năng phản ứng kịp thời của doanh nghiệp với các yêu cầu sản xuất. Dữ liệu này cũng làm tăng lợi ích thu được nhờ hiệu quả tiêu thụ năng lượng và tài nguyên. Dữ liệu người dùng, người tiêu dùng và nhà cung cấp rất quan trọng để phát triển kiến thức về thị trường, cải thiện khả năng tùy chỉnh và định hình các sản phẩm và mô hình kinh doanh mới. Khối lượng dữ liệu được tạo ra trên toàn cầu theo dự báo, sẽ tăng từ 33 zettabyte năm 2018 lên 175 zettabyte vào năm 2025, dẫn đến tốc độ tăng trưởng kép hàng năm là 61%.

Trong bối cảnh này, DNVVN phải bảo vệ dữ liệu theo cách phù hợp hơn. DNVVN thường có đặc quyền giữ bí mật thương mại như là phương thức bảo vệ dữ liệu mặc định. Bí mật thương mại là thông tin kinh doanh bí mật như các quy trình sản xuất mới, công thức cải tiến, kế hoạch kinh doanh hoặc thông tin thương mại về nhà cung cấp và danh sách khách hàng. Không giống bằng sáng chế, bí mật thương mại được luật pháp bảo vệ thông tin bí mật, ví dụ, thỏa thuận bảo mật hoặc không tiết lộ hoặc các điều khoản giao ước không cạnh tranh. Tính phổ biến của bí mật thương mại bắt nguồn từ khả năng dễ sử dụng (do đặc tính kỹ thuật thấp và thiếu các yêu cầu đăng ký chính thức), chi phí quản lý thấp và không có thời hạn bảo hộ xác định.

Số hóa gây khó khăn cho việc bảo vệ bí mật thương mại. Cuộc cách mạng mã hóa, lưu trữ và trao đổi dữ liệu (tức là ĐTĐM, email, ổ USB) là những động lực chính làm gia tăng các hành vi xâm phạm bí mật kinh doanh. Gia tăng giá trị là nhờ tài sản trí tuệ, sự di chuyển của người lao động và thay đổi văn hóa làm việc và các mối quan hệ (ví dụ, hợp đồng ngắn hạn, hỗ trợ tìm việc cho người lao động (outplacement), làm việc từ xa) hoặc sự phân khúc của chuỗi giá trị toàn cầu (với nhiều đối tác nước ngoài tham gia vào khuôn khổ pháp lý đa dạng và các điều kiện thực thi không đồng đều) cũng góp phần làm tăng nguy cơ tiết lộ thông tin.

*Cuộc khủng hoảng COVID-19 tạo cơ hội cho những kẻ xấu tăng cường tấn công*

Đại dịch COVID-19 năm 2020 đã khiến các doanh nghiệp phải xem xét lại mô hình kinh doanh. Các doanh nghiệp nhỏ chuyên bán lẻ, sản xuất và cung cấp một loạt các dịch vụ, hoạt động theo phương thức truyền thống trong đó phổ biến là tiếp xúc xã hội, đã phải đối mặt với nhu cầu giao hàng và kinh doanh theo cách “không tiếp xúc” hay dừng các hoạt động tại chỗ trong thời gian ngắn hoặc lâu dài. Cơ hội kinh doanh cũng xuất hiện trong bối cảnh khó khăn này.

Một số công nghệ và công cụ số đủ tiên tiến và hợp lý để cung cấp các giải pháp khả thi trong bối cảnh này. Các doanh nghiệp hiện đã sắp xếp lại cơ cấu tổ chức và quy trình hoạt động, điều chỉnh phương thức hoạt động, đề xuất các sản phẩm và/hoặc dịch vụ mới (như cửa hàng điện tử, giao hàng tận nhà ...), đồng thời tăng tốc áp dụng kỹ thuật số, trong khi khách hàng và người lao động của doanh nghiệp đều ở nhà.

DNVVN đi đầu thực hiện những điều chỉnh này vì bị ảnh hưởng nặng nề nhất của cuộc khủng hoảng. Quá trình chuyển đổi số trong doanh nghiệp đã diễn ra đôi khi không có sự hỗ trợ của kinh nghiệm kỹ thuật số cũ hay mức độ trưởng thành hoặc sự chuẩn bị rất ít về mặt kỹ thuật số.

Làm việc từ xa đã trở thành phương thức phổ biến rộng rãi trong đại dịch, mặc dù có sự khác nhau giữa và trong các quốc gia. Ví dụ, trước đại dịch, một nghiên cứu năm 2016 của Thụy Điển cho thấy “làm việc từ xa đã trở thành thói quen đối với hơn 20% tổng số lao động của nước này”. Theo một nghiên cứu năm 2017 trên 30 quốc gia châu Âu, 23% người Đan Mạch, 21% người Hà Lan và 18% người Thụy Điển làm việc tại nhà “ít nhất vài lần một tháng”. Tỷ lệ làm việc tại nhà thấp nhất là 6% ở cả Bulgaria và quốc đảo Síp. Các quốc gia OECD được xếp hạng thấp nhất là Cộng hòa Slovakia (8%) và Lithuania (8%). Ở Mỹ, ước tính có khoảng 7% lao động của ngành công nghiệp tư nhân và 4% cán bộ nhà nước và địa phương có lựa chọn làm việc từ xa. Một nghiên cứu gần đây của OECD khám phá sự đa dạng của các nhiệm vụ được thực hiện trong các loại nghề nghiệp khác nhau và sự phân bố theo địa lý của những nghề đó. Kết quả cho thấy các thành phố có tỷ lệ lao động làm việc từ xa cao hơn, dao động từ 50% ở Luxembourg đến 21% ở Thổ Nhĩ Kỳ; trong hầu hết các trường hợp, các thủ đô có tỷ lệ việc làm cao nhất trong các ngành nghề có thể thực hiện được từ xa.

Zoom, nền tảng hội nghị trực tuyến, đã có số người dùng hàng ngày tăng từ 10 triệu lên khoảng 200 triệu người trong ba tháng sau khi nhu cầu làm việc từ xa cao hơn. Đây là bước nhảy vọt cao nhất trong các nền tảng hội nghị truyền hình được sử dụng phổ biến. Tuy nhiên, các dịch vụ tương tự khác cũng có sự gia tăng nhanh chóng và mạnh mẽ nền tảng người dùng. Mỗi dịch vụ có các tính năng bảo mật khác nhau, bao gồm mã hóa đầu cuối, có nghĩa là bảo mật của người dùng khác nhau tùy thuộc vào dịch vụ và phương thức sử dụng.

Trên thực tế, cuộc khủng hoảng COVID-19 đã thu hút DNVVN và các tổ chức nhỏ như chính quyền địa phương chú ý đến hiện trạng bảo mật kỹ thuật số còn yếu của họ. Giống như các doanh nghiệp lớn, DNVVN buộc phải chuyển sang làm việc từ xa, đôi khi chỉ trong một thời gian nhất định. Sự thay đổi này đã làm tăng khả năng bị tấn công và tạo ra các lỗ hổng mới. Ví dụ, nhiều DNVVN không có Mạng riêng ảo (VPN), không sử dụng xác thực đa yếu tố để truy cập từ xa hoặc phải cho phép người lao động sử dụng thiết bị cá nhân nên không an toàn như thiết bị được cung cấp bởi đơn vị.

## **2.2. Quản lý rủi ro kỹ thuật số**

*Bộ công cụ bảo mật kỹ thuật số của các doanh nghiệp nhỏ ít mang tính toàn diện và tinh vi*

*Các doanh nghiệp nhỏ ít triển khai các biện pháp bảo mật kỹ thuật số*

Việc áp dụng các biện pháp bảo mật kỹ thuật số và quy mô doanh nghiệp có mối quan hệ chặt chẽ với nhau. Khi các doanh nghiệp có quy mô lớn hơn, thì họ sẽ

áp dụng nhiều biện pháp bảo mật kỹ thuật số tiên tiến hơn. Số liệu thống kê quốc gia cho kết quả tương tự:

- Một cuộc khảo sát riêng được thực hiện tại Vương quốc Anh chỉ ra rằng tỷ lệ các doanh nghiệp có chính sách chính thức về các rủi ro an ninh mạng tăng lên khi quy mô doanh nghiệp lớn hơn. Xu hướng này được lặp lại trong kết quả khảo sát của hai năm trước (2018 và 2017).

- Một nghiên cứu năm 2018 về Bảo mật CNTT và Quản lý dữ liệu trong DNVVN của Đan Mạch do Cục Doanh nghiệp Đan Mạch thực hiện, đã phát hiện ra mối quan hệ rõ ràng giữa quy mô doanh nghiệp (theo số lượng lao động) và các biện pháp bảo mật kỹ thuật số được áp dụng. Khi số lượng lao động tăng, tỷ lệ các doanh nghiệp thực hiện các biện pháp an ninh cơ bản hoặc thiết yếu sẽ tăng lên.

- Bên ngoài châu Âu, khảo sát ABACUS năm 2009 tại Úc cho thấy tỷ lệ doanh nghiệp có một số hình thức chính sách bảo mật máy tính tăng lên khi quy mô doanh nghiệp lớn hơn.

- Khi đối chiếu với Khảo sát về Vi phạm bảo mật mạng tại Vương quốc Anh năm 2019, thì xu hướng này vẫn tồn tại theo thời gian. DNVVN ít có khả năng thực hiện 5 hoặc 10 biện pháp bảo mật kỹ thuật số được khuyến nghị như một phần của “Hướng dẫn 10 bước” của Chính phủ, được ban hành lần đầu tiên vào năm 2015.

#### *Các phương thức bảo mật kỹ thuật số tinh vi hơn trong các doanh nghiệp lớn*

Các phương thức bảo mật kỹ thuật số về CNTT&TT không giống nhau giữa các doanh nghiệp. Các cuộc khảo sát doanh nghiệp châu Âu về việc sử dụng CNTT&TT cho thấy tất cả các doanh nghiệp dường như tích cực tham gia ngăn chặn sao lưu dữ liệu đến vị trí riêng biệt và cập nhật thường xuyên phần mềm và hệ điều hành. Khi so sánh với các phương thức bảo mật kỹ thuật số khác, thì khoảng cách trong việc triển khai giữa các doanh nghiệp siêu nhỏ và doanh nghiệp lớn bị giới hạn. Về bảo vệ quyền truy cập, các doanh nghiệp siêu nhỏ thường sử dụng xác thực mật khẩu tương đối mạnh, giống như các doanh nghiệp lớn.

Tuy nhiên, các doanh nghiệp nhỏ có xu hướng bỏ cuộc khi chuyển sang phương pháp tiếp cận an ninh mạng phức tạp hơn (như VPN hoặc sinh trắc học) hoặc phương pháp tích hợp nhiều hơn an ninh mạng hoặc giám sát liên tục.

#### *Các doanh nghiệp nhỏ ít phụ thuộc vào người lao động cho các mục đích bảo mật kỹ thuật số*

Các doanh nghiệp nhỏ thường ít có cán bộ chuyên thực hiện các hoạt động liên quan đến bảo mật CNTT&TT. Ví dụ, trên toàn khu vực EU28, các hoạt động bảo mật tại hơn 80% doanh nghiệp lớn được thực hiện bởi chính cán bộ của họ so

với tỷ lệ gần 40% doanh nghiệp nhỏ. Đồng thời, các doanh nghiệp nhỏ có xu hướng thuê lao động bên ngoài thực hiện nhiệm vụ bảo mật kỹ thuật số thông qua ký hợp đồng với các nhà tư vấn/chuyên gia, giống như các doanh nghiệp lớn. Năm 2019, trên toàn khu vực EU28, 65% DNVVN và 68% doanh nghiệp lớn có các hoạt động bảo mật CNTT&TT được thực hiện bởi các nhà cung cấp bên ngoài.

Một cách khác mà các doanh nghiệp ủy thác rõ ràng trách nhiệm bảo mật kỹ thuật số cho các bên thứ ba là thông qua các sản phẩm hoặc dịch vụ mà họ lựa chọn sử dụng. Ví dụ, sử dụng phần mềm thương mại như Microsoft Office, Gmail, Salesforce hoặc Adobe. Phần mềm và phần cứng được thiết kế rất cụ thể, bao gồm chức năng cơ bản của sản phẩm hoặc dịch vụ và/hoặc các tính năng bảo mật. Khi các doanh nghiệp lựa chọn sử dụng các sản phẩm hoặc dịch vụ này, họ đang ngầm giao một phần trách nhiệm cho nhà thiết kế, nhà sản xuất và/hoặc nhà bán lẻ cuối cùng. Sự ủy quyền này có hiệu quả trong trường hợp bên thứ ba có khả năng đưa ra các lựa chọn thiết kế phức tạp hơn và sử dụng nhiều nguồn lực hơn trong việc thiết kế và duy trì các tính năng bảo mật. Ví dụ, dịch vụ Đám mây, tận dụng các hiệu ứng mạng giữa những người dùng dịch vụ để cung cấp một bộ tính năng bảo mật tốt hơn so với khi người dùng cá nhân tự bảo vệ. Ngược lại, sự ủy quyền này không tối ưu trong trường hợp người dùng cuối không thể chắc chắn về chất lượng hoặc sức mạnh của các tính năng bảo mật khi không có kiến thức/thông tin chuyên môn.

*Các doanh nghiệp nhỏ cập nhật chính sách bảo mật CNTT&TT không thường xuyên*

Dữ liệu tương tự cung cấp một số thông tin chi tiết về tần suất các doanh nghiệp xem xét lại chính sách CNTT&TT của họ hoặc đã thiết kế chính sách hiện hành. Mặc dù các doanh nghiệp ở mọi quy mô gần đây đã sửa đổi chính sách CNTT&TT, nhưng tỷ lệ doanh nghiệp nhỏ làm điều này, vẫn thấp hơn hai lần so với các doanh nghiệp vừa và thấp hơn ba lần so với các doanh nghiệp lớn.

*DNVVN có xu hướng đầu tư ít hơn vào bảo mật kỹ thuật số*

DNVVN thường đầu tư ít hơn vào bảo mật kỹ thuật số so với các doanh nghiệp lớn, một phần là do xu hướng sử dụng công nghệ kỹ thuật số ít hơn. Tuy nhiên, chi tiêu cũng có xu hướng khác biệt với số ít doanh nghiệp cần sử dụng kỹ thuật số nhiều hơn trong một số lĩnh vực nhất định (như tài chính, thông tin, chăm sóc sức khỏe) có mức chi mỗi năm cho bảo mật kỹ thuật số (do sự cần thiết) nhiều hơn so với các doanh nghiệp trong các ngành ít dùng đến kỹ thuật số (như khách sạn, bất động sản, xây dựng). Một yếu tố cần lưu ý theo Khảo sát vi phạm mạng của Vương quốc Anh năm 2019, đó là tỷ lệ lớn doanh nghiệp nhỏ tuyên bố không chi cho bảo mật kỹ thuật số khi so sánh với các doanh nghiệp lớn.

Ngành công nghiệp chính sách bảo hiểm đang phát triển nhằm mục đích bù đắp các chi phí và tổn thất liên quan đến các sự cố bảo mật kỹ thuật số. Theo Moody's, dựa trên dữ liệu tài chính của Hoa Kỳ, phí bảo hiểm an ninh mạng trực tiếp đã tăng lên 2 tỷ USD vào năm 2018 hoặc tỷ lệ tăng trưởng tích lũy hàng năm là 26% kể từ năm 2015 (Moody's, 2019). Quy định chung về bảo vệ dữ liệu (GDPR) của EU được kỳ vọng sẽ giúp thúc đẩy tăng trưởng nhanh hơn ở châu Âu sau khi được thực thi vào năm 2018.

Tuy nhiên, DNVVN có xu hướng mua các chính sách bảo hiểm bảo mật kỹ thuật số mang tính độc lập ít hơn các doanh nghiệp lớn. Đây là điểm chung của tất cả các quốc gia tham gia khảo sát của châu Âu về sử dụng CNTT&TT, ngoại trừ Đan Mạch. Tại EU28, trung bình có khoảng 40% doanh nghiệp lớn mua bảo hiểm CNTT&TT, trong khi DNVVN là 20%.

Ngoài lý do nhiều chính sách bảo hiểm không độc lập có thể được kích hoạt trong trường hợp xảy ra một số sự cố bảo mật kỹ thuật số (ví dụ, thiệt hại tài sản và đường dây hồng học do mã độc kích hoạt), thì có một số lý do DNVVN thường mua loại bảo hiểm này nhiều hơn doanh nghiệp lớn. Khi được khảo sát vào năm 2019 về lý do doanh nghiệp không mua “bảo hiểm mạng”, những người được hỏi ở Vương quốc Anh đã trả lời như sau:

- Họ đã được cung cấp bởi một nhà cung cấp an ninh mạng bên ngoài (23% doanh nghiệp và 26% tổ chức từ thiện).
- Họ thiếu nhận thức về bảo hiểm mạng (23% doanh nghiệp và 15% tổ chức từ thiện).
- Họ tự cho là có rủi ro quá thấp (29% tổ chức từ thiện và 22% doanh nghiệp)

*Có sự khác biệt lớn giữa các quốc gia về cách DNVVN bảo mật hệ thống và dữ liệu*

Việc triển khai các biện pháp và phương thức bảo mật kỹ thuật số theo quốc gia có sự khác biệt đáng kể. Ở hầu hết các quốc gia được khảo sát trong khuôn khổ cuộc điều tra Cộng đồng năm 2015 về sử dụng CNTT&TT trong doanh nghiệp, khi được hỏi liệu doanh nghiệp có áp dụng chính sách CNTT&TT chính thức hay không, thì tỷ lệ khác biệt giữa DNVVN và các doanh nghiệp lớn khoảng 30%. Các kết quả này đã được củng cố trong cuộc khảo sát năm 2019 gần đây nhất.

### 2.3. Các chính sách công tăng cường quản lý rủi ro kỹ thuật số

Do DNVVN quản lý rủi ro bảo mật kỹ thuật số theo cách riêng và hậu quả kinh tế của việc quản lý kém hiệu quả rủi ro bảo mật kỹ thuật số của các doanh nghiệp, nên chính phủ nhiều nước OECD đã triển khai thực hiện nhiều chính sách khác nhau. Trên thực tế, DNVVN chiếm gần 99% tổng số doanh nghiệp ở hầu hết



các quốc gia OECD, do đó, bất kỳ sáng kiến nào của chính phủ nhằm cải thiện bảo mật kỹ thuật số trong doanh nghiệp đều sẽ được áp dụng và/hoặc ảnh hưởng đến DNVVN. Số ít quốc gia OECD đã áp dụng các chính sách dành riêng cho DNVVN nhằm cải thiện bảo mật kỹ thuật số theo nhiều cách khác nhau.

### *Tìm hiểu cơ sở lý luận của can thiệp chính sách*

Trước tiên, chính phủ các nước đóng vai trò quan trọng trong việc duy trì các khuôn khổ pháp lý và tư pháp, trong đó có hoạt động hành chính công và thị trường, cũng như hạn chế việc chiếm đoạt dữ liệu, vi phạm tài sản và quyền riêng tư, gian lận và tống tiền. Điều này rất quan trọng vì DNVVN bị ảnh hưởng không đồng đều bởi các thể chế và khung pháp lý kém hiệu quả.

Ngoài ra, rủi ro bảo mật kỹ thuật số một phần là hậu quả của nhiều thất bại trong thị trường công nghệ số. Theo đó, chính phủ các nước có thể cung cấp các điều kiện để thị trường đạt được mức độ an toàn kỹ thuật số tối ưu về mặt xã hội, coi an ninh mạng có các đặc điểm của hàng hóa công. Những thất bại của thị trường bao gồm:

- Bất cân xứng thông tin giữa người tiêu dùng: Người tiêu dùng khó đánh giá các tính năng bảo mật của các sản phẩm kỹ thuật số cao, cũng như chất lượng tương đối của mã phần mềm, vì thiếu năng lực kỹ thuật và vì nhiều nhà sản xuất sử dụng biện pháp bảo vệ để ngăn chặn kiểm tra phần mềm. Khi cân nhắc mua sản phẩm nào đó, người tiêu dùng không phải lúc nào cũng có thể đánh giá được đâu mới thực sự là lựa chọn an toàn hơn.

- Sự bóp méo của các tín hiệu thị trường đối với nhà sản xuất: Vấn đề phức tạp là người tiêu dùng không có khả năng đánh giá mức độ an toàn tương đối của một sản phẩm, có nghĩa là nhà sản xuất đã đầu tư vào các sản phẩm an toàn hơn, lại không thể dễ dàng phân biệt chúng trên thị trường. Điều này ngăn họ chuyển chi phí phát triển bảo mật bổ sung cho người dùng cuối, ví dụ, dưới dạng phí bảo hiểm giá, cũng dẫn đến sự xuất hiện của “thị trường lemon”, nơi các sản phẩm “tốt” bị những sản phẩm “xấu” lấn át. Do đó, đầu tư tư nhân vào bảo mật kỹ thuật số có thể thấp hơn mức xã hội mong đợi nếu các doanh nghiệp không thể thu được lợi nhuận từ các khoản đầu tư.

- Các yếu tố bên ngoài tiêu cực: Chi phí cho các sự cố bảo mật kỹ thuật số không phải lúc nào cũng do nhà sản xuất công nghệ gánh. Hơn nữa, một số nhà sản xuất không áp dụng các biện pháp bảo mật đầy đủ để giảm xác suất xảy ra một số sự cố, vì chi phí khắc phục sự cố do những người khác chịu. Một lần nữa, các yếu tố bên ngoài tiêu cực có thể dẫn đến việc đầu tư quá mức vào bảo mật kỹ thuật số.

- **Rủi ro đạo đức:** Rủi ro đạo đức làm tăng bất ổn vì liên quan đến việc một bên phải chịu chi phí và tổn thất cho các hành động rủi ro của người khác.

*Các sáng kiến gần đây của các nước nhằm cải thiện các phương thức bảo mật kỹ thuật số cho DNVVN*

Cho đến nay, nỗ lực của chính phủ các nước nhằm khuyến khích sản xuất các sản phẩm kỹ thuật số an toàn hơn (“bảo mật theo thiết kế” hoặc “quyền riêng tư theo thiết kế”) và đưa ra các hình phạt với các đối tượng có những sản phẩm dẫn đến sự cố bảo mật kỹ thuật số hoặc không quản lý đúng cách rủi ro bảo mật kỹ thuật số gây mất chi phí hoặc tổn thất cho các bên khác. Nhiều sáng kiến trong số đó đã được thực hiện như một phần hoặc sau khi áp dụng các chiến lược an ninh mạng tại các quốc gia OECD. Số lượng sáng kiến tăng lên theo thời gian.

Các chiến lược bảo mật kỹ thuật số quốc gia bao gồm các chính sách liên quan và theo Khuyến nghị của OECD, nên đưa DNVVN tham gia vào thiết kế và thực hiện chính sách (Bảng 8).

*Bảng 8. Lồng ghép các cân nhắc chính sách DNVVN trong các chiến lược bảo mật kỹ thuật số quốc gia*

Quốc gia	Chiến lược quốc gia	Sự tham gia của DNVVN vào thiết kế	Sự tham gia của DNVVN vào thực hiện
Braxin	Chiến lược An ninh mạng quốc gia (2019-2023)		
Canada	Chiến lược An ninh mạng quốc gia Canada, Tầm nhìn của Canada về An ninh và Thịnh vượng trong Kỷ nguyên số (2010-2024)	Có	Có
Colombia	Chính sách An ninh số quốc gia (2016-2020)		
Đan Mạch	Chiến lược An ninh mạng và Thông tin (2018-2021)	Có	Có
Phần Lan	Chiến lược An ninh mạng Phần Lan (2013-2020)		
Nhật Bản	Chiến lược An ninh mạng (2018-2021)		
Mexico	Chiến lược An ninh mạng quốc gia (2017-2018)		
Hà Lan	Chương trình An ninh mạng quốc gia (2018)	Có	Có
Tây Ban Nha	Chiến lược An ninh mạng quốc gia (2019-2024)		Có
Thụy Điển	Chiến lược số (tháng 5/2017), Chiến lược	Có	

	An ninh mạng quốc gia (tháng 6/2017)		
Thổ Nhĩ Kỳ	Chiến lược An ninh mạng quốc gia (2016-2019)		
Hoa Kỳ	Chiến lược An ninh mạng quốc gia (2018)	Có	Có

*Nguồn: Phản ứng của các quốc gia trong Khảo sát của OECD về Chính sách bảo mật kỹ thuật số năm 2019*

Các sáng kiến của chính phủ nhằm cải thiện mức độ bảo mật kỹ thuật số tổng thể trên các thị trường có thể phân thành những loại sau. Một là các chính sách khuyến khích doanh nghiệp cung cấp các giải pháp bảo mật kỹ thuật số hiện có/mới (bên cung), hoặc hai là các chính sách khuyến khích doanh nghiệp cải thiện việc áp dụng các phương thức quản lý rủi ro bảo mật kỹ thuật số hiệu quả hơn (bên cầu) (Bảng 9).

*Bảng 9. Các ví dụ được chọn lọc về các sáng kiến chính sách nhằm tăng cường bảo mật kỹ thuật số trong khu vực DNVVN*

Mục tiêu chiến lược	Công cụ chính sách	Ví dụ từ các quốc gia
<b>Bên cung: Khuyến khích cung cấp các giải pháp bảo mật kỹ thuật số cho doanh nghiệp</b>		
Tăng cường các tính năng "an ninh theo thiết kế" hoặc "bảo mật theo thiết kế" cho các sản phẩm CNTT	Quy định và pháp luật	<ul style="list-style-type: none"> <li>Các yêu cầu bắt buộc về bảo mật trong Dự luật SB-327 California cho các thiết bị kết nối</li> </ul>
Giảm chi phí giao dịch thương mại, kể cả ở nước ngoài	Tiêu chuẩn bảo mật	<ul style="list-style-type: none"> <li>Đạo luật An ninh mạng của EU</li> <li>Khung an ninh mạng NIST của Hoa Kỳ</li> </ul>
Phát triển các công nghệ bảo mật kỹ thuật số mới thông qua DNVVN	Trợ cấp, tín dụng thuế, cụm và các cơ chế tài chính khác	<ul style="list-style-type: none"> <li>Kế hoạch Kỹ năng và Đổi mới của Canada</li> <li>Chương trình PROSOFT của Mexico</li> </ul>
<b>Bên cầu: Khuyến khích áp dụng các phương pháp bảo mật kỹ thuật số hiệu quả hơn trong doanh nghiệp</b>		
Đưa ra các quy tắc và hướng dẫn quản lý dữ liệu	Quy định và pháp luật	<ul style="list-style-type: none"> <li>Quy định chung và Chỉ thị về bảo vệ dữ liệu của EU (GDPR) và Khuôn khổ thực hiện trên toàn quốc</li> <li>Đạo luật về quyền riêng tư của người tiêu dùng California</li> </ul>
Đặt ra các quy tắc và yêu cầu	Quy định và pháp luật	<ul style="list-style-type: none"> <li>Luật năm 2017 về dữ liệu công</li> </ul>

cho Quy định bản địa hóa dữ liệu	luật	dân Trung Quốc
Tăng sự khác biệt về thị trường và giá cao hơn cho các phương thức tốt	Các chương trình chứng nhận	<ul style="list-style-type: none"> <li>• Chương trình Chứng nhận CyberSecure Canada và CyberSecure Canada Logo</li> </ul>
Giảm sự bất cân xứng thông tin cho những người tiếp nhận	Các tiêu chuẩn và thủ tục bảo mật	<ul style="list-style-type: none"> <li>• Chương trình Cyber Essential Plus của Anh</li> <li>• Đạo luật An ninh mạng EU</li> </ul>
Nâng cao năng lực của doanh nghiệp theo hướng quản lý rủi ro kỹ thuật số	Dịch vụ phát triển kinh doanh và nguồn lực thông tin	<ul style="list-style-type: none"> <li>• Đạo luật An ninh mạng cho DNVVN của Hoa Kỳ</li> <li>• Chương trình “Dừng lại. Nghĩ. Kết nối” của Hoa Kỳ</li> </ul>
Xây dựng văn hóa và kỹ năng an ninh mạng		
Giáo dục và đào tạo	Cung cấp tài liệu giáo dục, hội nghị, đào tạo	<ul style="list-style-type: none"> <li>• Bộ công cụ Get Cyber Safe của Canada</li> <li>• Kế hoạch Phát triển nguồn nhân lực an ninh mạng của Nhật Bản</li> <li>• Các chương trình của Cơ quan An ninh mạng của Hàn Quốc</li> <li>• Sáng kiến quốc gia về Giáo dục an ninh mạng của Hoa Kỳ</li> </ul>
Xây dựng nền tảng kiến thức về các rủi ro bảo mật kỹ thuật số và tài liệu giáo dục	Nhóm xử lý sự cố bảo mật máy tính	Úc, Áo, Đan Mạch, Hàn Quốc
Nâng cao nhận thức về rủi ro bảo mật kỹ thuật số và các phương thức tốt	Chiến dịch nâng cao nhận thức	<ul style="list-style-type: none"> <li>• Tháng an ninh mạng (Canada, Chile, EU)</li> <li>• Các chiến dịch quốc gia (Mexico, Vương quốc Anh, Hoa Kỳ)</li> </ul>

### *Luật bảo mật kỹ thuật số*

Trong những năm gần đây, nhiều nước đã nỗ lực xây dựng và thực hiện luật tăng cường bảo mật kỹ thuật số. Đôi khi, những nỗ lực pháp lý này chòng chẹo với nỗ lực bảo vệ dữ liệu và quyền riêng tư nhưng có thể được coi là khác biệt do các mục tiêu và cấu trúc khác nhau. Các luật bảo mật kỹ thuật số quốc gia thường nhằm tăng cường bảo mật kỹ thuật số trong các tổ chức của khu vực công và thành lập các tổ chức thuộc khu vực công mới chịu trách nhiệm bảo mật kỹ thuật số, mặc dù trong một số trường hợp, các quy định của họ cũng áp dụng cho các doanh nghiệp của khu vực tư nhân hoặc ảnh hưởng đến các doanh nghiệp này.

Nỗ lực pháp lý liên bang đáng chú ý gần đây nhất liên quan đến bảo mật kỹ thuật số ở Hoa Kỳ là Đạo luật An ninh mạng cho DNVVN của Viện Tiêu chuẩn và Công nghệ quốc gia (NIST). Quy định này được chuyển thành luật vào tháng 8 năm 2018, yêu cầu NIST “cung cấp các nguồn lực thông tin rõ ràng và ngắn gọn để giúp các doanh nghiệp nhỏ quan tâm đến việc xác định, đánh giá, quản lý và giảm thiểu rủi ro an ninh mạng”. Các nguồn thông tin này thường được dùng cho nhiều loại hình doanh nghiệp nhỏ; thay đổi theo bản chất và quy mô của các doanh nghiệp nhỏ; nâng cao nhận thức về an ninh mạng và văn hóa an ninh mạng tại nơi làm việc; và bao gồm các chiến lược ứng dụng thực tế.

Tuy nhiên, một ví dụ đáng chú ý về DNVVN là Dự luật SB-327 của California “Quyền riêng tư về thông tin: thiết bị được kết nối” quy định “yêu cầu nhà sản xuất bán hoặc chào bán thiết bị kết nối ở California phải trang bị cho thiết bị kết nối một hoặc nhiều tính năng bảo mật hợp lý phù hợp với bản chất và chức năng của thiết bị thiết kế để bảo vệ thiết bị khỏi bị truy cập hoặc sử dụng trái phép từ xa”. Dự luật này rất đáng chú ý vì quy định các biện pháp bảo mật cụ thể phải được thực hiện trong thiết bị IoT, khác biệt hoàn toàn so với xu hướng của các nhà lập pháp ở hầu hết các khu vực pháp lý để tránh luật quy định bắt buộc một số tính năng bảo mật nhất định.

Trong những năm gần đây, một đạo luật quốc gia mang tính hệ quả trong lĩnh vực bảo mật kỹ thuật số đã được thực hiện ở Trung Quốc. Luật có hiệu lực vào tháng 6 năm 2017, áp đặt các yêu cầu mới về bảo mật kỹ thuật số và quản lý dữ liệu đối với các doanh nghiệp thực hiện kinh doanh trong nước và với các tổ chức đặt trụ sở tại Trung Quốc. Một nội dung mang tính hệ quả của luật này đối với DNVVN liên quan đến các yêu cầu bản địa hóa dữ liệu. Nếu một doanh nghiệp hoạt động ở Trung Quốc và thu thập thông tin cá nhân của công dân Trung Quốc, thì doanh nghiệp đó bắt buộc phải lưu trữ dữ liệu đó trên các máy chủ đặt tại Trung Quốc. Nếu các doanh nghiệp cho rằng việc chuyển thông tin đó ra nước ngoài “do yêu cầu kinh doanh” là “cần thiết”, thì việc chuyển giao chỉ được thực hiện sau khi đánh giá khía cạnh bảo mật. Hậu quả là gây khó khăn và tốn kém cho các doanh nghiệp nước ngoài hoạt động tại Trung Quốc.

Đây là một phần của xu hướng lớn bản địa hóa dữ liệu, vốn đang làm tăng chi phí tương tự như hoạt động kinh doanh ở một số quốc gia khác. Các ví dụ khác bao gồm Úc, Đức, Thổ Nhĩ Kỳ, Liên bang Nga và Hàn Quốc. Tác động tiềm tàng của các yêu cầu về bản địa hóa dữ liệu đối với DNVVN nên được hiểu là sự gia tăng của các dịch vụ mới như dữ liệu lớn, ĐTDĐ và IoT. Nhiều nhà cung cấp các dịch vụ này hoạt động trên phạm vi quốc tế; do đó, các yêu cầu bản địa hóa dữ liệu có thể làm tăng rào cản gia nhập và không khuyến khích những người mới tham

gia thị trường. Do đó, DNVVN địa phương sẽ phải đối mặt với sự gia tăng đáng kể chi phí tính toán, có thể lên tới 30-60%.

#### *Các chương trình chứng nhận và tiêu chuẩn bảo mật*

Một số quốc gia đã bắt đầu triển khai các chương trình chứng nhận quốc gia về bảo mật kỹ thuật số. Các sáng kiến này liên quan đến nhiều “phương thức tốt nhất” mà doanh nghiệp có thể áp dụng trong hoạt động hoặc trong việc thiết kế các sản phẩm và dịch vụ. Sau khi hoàn thành các bước cần thiết, doanh nghiệp được cấp chứng nhận, có thể thông báo cho người tiêu dùng hoặc đối tác kinh doanh về mức độ bảo mật kỹ thuật số của doanh nghiệp hoặc các sản phẩm/dịch vụ của doanh nghiệp. Các kế hoạch này nhằm tăng danh tiếng của doanh nghiệp và giảm sự bất cân xứng về thông tin trên thị trường. Các chương trình đó cũng có thể khuyến khích các nhà sản xuất thiết kế sản phẩm/dịch vụ của họ theo cách “an toàn theo thiết kế”. Bằng cách này, các kế hoạch dán nhãn giúp các nhà cung cấp biến bảo mật thành một lợi thế cạnh tranh và hỗ trợ tạo sự khác biệt trên thị trường.

Đạo luật An ninh mạng của EU đưa ra “một khuôn khổ chứng nhận an ninh mạng trên toàn EU cho các sản phẩm, dịch vụ và quy trình CNTT&TT”. Khuôn khổ này vẫn đang trong quá trình phát triển, nhằm cung cấp một bộ quy tắc, yêu cầu kỹ thuật, tiêu chuẩn và thủ tục toàn diện để đánh giá các đặc tính bảo mật của một sản phẩm hoặc dịch vụ dựa vào CNTT&TT. Điều đó có thể mang lại lợi ích cho DNVVN, trong đó, cung cấp một tiêu chuẩn được thống nhất chung và rõ ràng hơn về bảo mật kỹ thuật số đối với các sản phẩm/dịch vụ.

Một chương trình chứng nhận chung hoặc nhất quán giữa các quốc gia cũng đi kèm với các lợi ích bổ sung: người tiêu dùng có thể tham khảo một tiêu chuẩn đáng tin cậy và dễ nhận biết, trong khi các nhà sản xuất được hưởng lợi từ việc giảm chi phí giao dịch và cơ hội liên quan đến hoạt động xuyên biên giới, cũng sẽ làm tăng lợi nhuận cho sản phẩm.

Trong một nội dung của Chương trình An ninh mạng quốc gia, Vương quốc Anh đã xây dựng và triển khai các chương trình Cyber Essentials và Cyber Essentials Plus. Các chương trình này bao gồm một khuôn khổ đảm bảo và một tập hợp các biện pháp kiểm soát bảo mật đơn giản mà doanh nghiệp có thể thực hiện để bảo vệ dữ liệu và hệ thống khỏi các mối đe dọa từ môi trường mạng. Cyber Essentials là công cụ tự đánh giá, được xác minh độc lập. Ngược lại, Cyber Essentials Plus liên quan đến thử nghiệm độc lập.

Sáng kiến tương tự là Chương trình Chứng nhận CyberSecure của Canada, được công bố vào tháng 8 năm 2019. “DNVVN tuân thủ các biện pháp kiểm soát an ninh mạng cụ thể, dựa trên đánh giá của một tổ chức cấp chứng nhận được công

nhận, sẽ được cấp chứng nhận hai năm và có quyền sử dụng logo của CyberSecure Canada”.

### *Đổi mới các công nghệ bảo mật kỹ thuật số*

DNVVN có thể là nguồn cung cấp các sản phẩm, dịch vụ hoặc phương thức bảo mật kỹ thuật số mới và cải tiến. Chính phủ các nước có thể thúc đẩy đổi mới bảo mật kỹ thuật số trong các doanh nghiệp, trong đó có DNVVN, bằng các biện pháp như ưu đãi thuế, đóng vai trò là khách hàng đầu tiên cho các sản phẩm sáng tạo, sử dụng quy định để kích thích nhu cầu đối với các sản phẩm đó hoặc tạo ra hệ sinh thái đổi mới bảo mật kỹ thuật số.

Kế hoạch Kỹ năng và Đổi mới của Canada khuyến khích phát triển nhiều ngành công nghiệp đổi mới sáng tạo, bao gồm cả ngành “kỹ thuật số” trong đó có bảo mật kỹ thuật số. Mặc dù DNVVN không được đề cập cụ thể như một mục tiêu cho các sáng kiến này, nhưng kế hoạch sẽ có ý nghĩa đối với DNVVN thông qua việc tạo ra các siêu nhóm, thu hút các khoản đầu tư kinh doanh chất lượng cao mới (thông qua Quỹ Đổi mới chiến lược) và hỗ trợ các doanh nghiệp đổi mới nhờ đầu tư mạo hiểm.

Mexico, thông qua Chương trình PROSOFT lâu dài, thúc đẩy việc thành lập các Trung tâm đổi mới công nghiệp (IIC) tập trung vào cung cấp nguồn nhân lực được đào tạo và chuyên môn hóa, cũng như áp dụng các công nghệ mới liên quan đến “Công nghiệp 4.0”, như bảo mật kỹ thuật số.

Chiến lược An ninh mạng quốc gia của Tây Ban Nha nhằm tạo ra tri thức và phát triển các hoạt động nghiên cứu và phát triển trong lĩnh vực bảo mật kỹ thuật số. Chiến lược này đặc biệt tập trung vào, “củng cố ngành công nghiệp an ninh mạng của Tây Ban Nha và năng lực của quốc gia trong việc nuôi dưỡng và giữ chân nhân tài để tăng cường quyền tự chủ kỹ thuật số”. Trong số các biện pháp khác nhau được đề xuất là: thúc đẩy các chương trình hỗ trợ NC&PT trong lĩnh vực bảo mật kỹ thuật số tại DNVVN, loại hình doanh nghiệp khác, trường đại học và trung tâm nghiên cứu; tạo điều kiện tiếp cận các chương trình xúc tiến trong nước và quốc tế; và các chương trình mua sắm công sáng tạo.

Vương quốc Anh sử dụng hoạt động mua sắm công để khuyến khích DNVVN và các thành viên trong chuỗi cung ứng tăng cường bảo mật kỹ thuật số. Các doanh nghiệp muốn trở thành nhà cung cấp của chính phủ, cần phải thực hiện các chương trình chứng nhận Cyber Essentials hoặc Cyber Essentials Plus. Cách tiếp cận này thúc đẩy bảo mật kỹ thuật số mà không tạo ra các quy định tuân thủ cứng nhắc, có thể lỗi thời nhanh hoặc đặt ra các yêu cầu khắt khe đối với doanh nghiệp.

Tổ chức An ninh mạng châu Âu (ECISO), là quan hệ đối tác công-tư điều phối các lộ trình đổi mới và đầu tư ở Liên minh châu Âu. Tổ chức này tập hợp nhiều bên liên quan bao gồm DNVVN và rộng hơn là ngành công nghiệp, giới học giả, đại diện khu vực và các quốc gia thành viên. ECISO giúp ưu tiên đầu tư vào nhiều lĩnh vực kỹ thuật, trong đó có bảo mật kỹ thuật số.

### *Các chiến dịch giáo dục và nâng cao nhận thức*

Nhiều quốc gia đã nỗ lực để nâng cao nhận thức về bảo mật kỹ thuật số trong cộng đồng, đôi khi nhằm vào khu vực doanh nghiệp và DNVVN. Những nỗ lực đó nhằm đưa ra tư vấn /hướng dẫn có chất lượng và các giải pháp tương đối ít tốn kém, nếu được áp dụng, sẽ làm giảm đáng kể mức độ rủi ro về bảo mật kỹ thuật số cho DNVVN và các tổn thất tiềm ẩn.

Như một nội dung trong Chiến lược An ninh mạng 2020, Úc đã áp dụng một số sáng kiến dành riêng cho DNVVN, bao gồm một số sáng kiến liên quan đến các chiến dịch giáo dục và nâng cao nhận thức. Trung tâm An ninh mạng Úc (ACSC) đã lựa chọn cung cấp cả hướng dẫn về những gì DNVVN nên làm và cả phương thức thực hiện chiến lược bảo mật kỹ thuật số. Các ví dụ về chính sách bao gồm các bộ công cụ phù hợp (ví dụ: để đánh giá mức độ trưởng thành).

Cơ quan Dịch vụ công Liên bang Bỉ về Kinh tế, DNVVN, Tầng lớp trung lưu và Năng lượng có một bộ tài nguyên trực tuyến để cung cấp thông tin và hỗ trợ DNVVN các vấn đề bảo mật kỹ thuật số. Bộ công cụ này bao gồm tài liệu và các đánh giá rủi ro, các nguyên tắc chính để tăng cường bảo mật kỹ thuật số, những việc cần làm trong trường hợp xảy ra sự cố và bảng chú giải các thuật ngữ kỹ thuật chính.

Braxin đưa ra nhiều hoạt động như một phần nội dung của Chiến lược An ninh mạng nhằm "đưa ra các hành động nâng cao nhận thức về an ninh mạng cho DNVVN". Điều này giúp DNVVN tăng kỹ năng bảo mật kỹ thuật số và khả năng phục hồi của Braxin trước các mối đe dọa về bảo mật kỹ thuật số.

Trung tâm An ninh mạng Canada cung cấp cho mọi người bộ công cụ “An toàn không gian mạng” trong Tháng an ninh mạng (tháng 10). Chương trình giảng dạy có cấu trúc bao gồm các chủ đề như “Phương thức hoạt động của các mối đe dọa trên mạng”, “Cách các mối đe dọa trên mạng ảnh hưởng đến bạn” và “Cách bảo vệ doanh nghiệp nhỏ của bạn”.

Chính sách An ninh mạng quốc gia của Chile bao gồm việc thiết kế một chiến dịch an ninh mạng quy mô lớn để thúc đẩy việc thực hiện các chương trình phổ biến và nâng cao nhận thức với sự hợp tác của khu vực tư nhân. Tài liệu chính sách cũng đề cập đến tháng 10 là Tháng an ninh mạng và Ngày Internet an toàn



vào tháng 2 hàng năm. Ngoài ra, Bộ Giáo dục quản lý sáng kiến “Internet Segura” (Internet An toàn), giúp mọi người sử dụng Internet theo cách “có trách nhiệm, có hiểu biết, an toàn, đạo đức, miễn phí và có sự tham gia”.

Chiến lược An ninh mạng và Thông tin của Đan Mạch tập trung củng cố kiến thức về bảo mật CNTT nhờ có các chuyên gia tư vấn chính của DNVVN đóng vai trò là cầu nối. Mục đích là để các chuyên gia tư vấn này (như kế toán, luật sư ...) nêu ra các vấn đề về bảo mật CNTT trong cuộc đối thoại với lãnh đạo DNVVN.

Pháp đưa ra chương trình dán nhãn SecNumedu, cung cấp các khóa đào tạo chuyên nghiệp cho DNVVN. Đây là hướng dẫn phát triển môi trường an toàn cho máy tính và mạng tại DNVVN và một nền tảng báo cáo về các hoạt động độc hại và hỗ trợ cho các chuyên gia.

Nhật Bản đã thành lập Trụ sở Chiến lược An ninh mạng vào năm 2014 với một số trách nhiệm thực hiện “Kế hoạch phát triển nguồn nhân lực an ninh mạng”. Các chức năng tiếp cận cộng đồng bao gồm hợp tác với các thành viên Hiệp hội các quốc gia Đông Nam Á (ASEAN) về “nâng cao nhận thức và xây dựng năng lực”...

Cơ quan An ninh Internet của Hàn Quốc (KISA) cung cấp nhiều chương trình đào tạo chuyên nghiệp và giáo dục để nâng cao nhận thức của công chúng, mở rộng các khóa học về an ninh mạng trong giáo dục đại học và thúc đẩy việc cấp chứng nhận của các chuyên gia trong cả khu vực công và tư.

Mexico đưa ra Chiến lược An ninh mạng quốc gia và tiến hành các chiến dịch nâng cao nhận thức. Cảnh sát Liên bang điều hành Chiến dịch An ninh mạng Mexico, nhằm “nâng cao nhận thức trong xã hội Mexico về việc sử dụng có trách nhiệm các công nghệ mới và Internet để giảm thiệt hại do tội phạm mạng gây ra”. Ngoài ra, kể từ năm 2015, Tuần lễ An ninh mạng quốc gia được tổ chức với sự cộng tác của Tổ chức các Quốc gia châu Mỹ.

Năm 2018, Thụy Điển đã giao quyền phát triển và thực hiện một chương trình nhằm tăng cường kỹ năng số hóa cho ban quản lý và hội đồng quản trị của các doanh nghiệp nhỏ. Chương trình kéo dài 3 năm, giúp các doanh nghiệp nhỏ nâng cao năng lực đánh giá và quản lý rủi ro số hóa từ góc độ kinh tế.

Bộ An ninh Nội địa Hoa Kỳ (DHS) quản lý Sáng kiến Quốc gia về Giáo dục An ninh mạng, bao gồm bốn hoạt động chính: 1) Chiến dịch nâng cao nhận thức về an ninh mạng quốc gia, 2) giáo dục chính thức về an ninh mạng, 3) Cơ cấu lực lượng lao động về an ninh mạng liên bang và 4) Đào tạo Lực lượng lao động về an ninh mạng và Phát triển chuyên nghiệp. Chương trình “Dừng. Nghĩ. Kết nối” là chiến dịch nâng cao nhận thức cộng đồng của quốc gia nhằm tăng cường hiểu biết

về các mối đe dọa mạng và khuyến khích công chúng truy cập trực tuyến theo cách an toàn và bảo mật hơn. Một bộ công cụ đã được tập hợp cho các nhóm khác nhau, bao gồm cả ngành công nghiệp và các doanh nghiệp nhỏ.

Ủy ban Châu Âu và Cơ quan điều hành DNVVN (EASME), gần đây đã thực hiện sáng kiến hỗ trợ phát triển kỹ năng chuyên ngành về Dữ liệu lớn, IoT và An ninh mạng cho DNVVN châu Âu. Sáng kiến này liên quan đến việc triệu tập nhiều bên liên quan để thảo luận các vấn đề và đi đến một báo cáo cuối cùng phân tích những lợi ích và rào cản tiềm năng của DNVVN trong việc áp dụng công nghệ. Báo cáo đề cập đến tầm nhìn, lộ trình và hộp công cụ nhằm nâng cao năng lực của các ngành, các đối tác xã hội, các tổ chức giáo dục và đào tạo và các nhà hoạch định chính sách ở tất cả các cấp nhằm thúc đẩy và hỗ trợ các DNVVN ở châu Âu tích lũy các kỹ năng này.

## **KẾT LUẬN**

Trong quá trình thực hiện chuyển đổi số, các quốc gia chủ động tháo gỡ những rào cản mà DNVVN gặp phải, bao gồm thiếu thông tin và nhận thức, thiếu hụt kỹ năng, không đủ vốn, thiếu tài sản bổ sung như bản thân công nghệ hoặc các phương thức tổ chức hoặc khó thích ứng với sự thay đổi khung pháp lý, cũng như ứng phó với các vấn đề về bảo mật kỹ thuật số và bảo vệ dữ liệu, hoặc đơn giản là tiếp cận cơ sở hạ tầng kỹ thuật số có chất lượng. Trong khi một số quốc gia tìm cách lồng ghép các cân nhắc chính sách về DNVVN trong các chương trình chính sách khác, thì các quốc gia khác lại nhắm mục tiêu cụ thể đến các DNVVN bằng các công cụ được thiết kế riêng, thường được kết hợp với hỗn hợp chính sách theo địa điểm hoặc ngành.

Cuộc khủng hoảng COVID-19 đã nâng cao tầm quan trọng của chuyển đổi số trong DNVVN. Các doanh nghiệp đã chuyển sang hoạt động trực tuyến và triển khai các giải pháp làm việc thông minh để duy trì hoạt động kinh doanh trong thời gian phong tỏa và khắc phục sự gián đoạn trong chuỗi cung ứng, với các nền tảng trực tuyến đóng vai trò quan trọng kết nối người dùng với các thị trường, nhà cung cấp hoặc nguồn lực mới.

Tuy nhiên, bối cảnh COVID-19 cũng tạo cơ hội cho tin tặc tăng cường tấn công nhằm vào điểm yếu của DNVVN, đó là thiếu sự chuẩn bị để ứng phó với các mối đe dọa ngày càng tinh vi. Các sự cố bảo mật kỹ thuật số có thể gây ra tổn thất lớn và có xu hướng gia tăng theo quy mô doanh nghiệp. Một tỷ lệ nhỏ các doanh nghiệp đã gặp sự cố và chịu nhiều tổn thất. Đôi khi, DNVVN có thể phải chịu tổn

thất cao bằng vài tháng doanh thu. Ngoài ra, các phương thức bảo mật kỹ thuật số yếu kém có thể là rào cản đối với DNVVN xây dựng mạng lưới kinh doanh.

DNVVN thường có ít các phương thức quản lý rủi ro bảo mật kỹ thuật số toàn diện và phức tạp hơn. Doanh nghiệp thường không có người chuyên trách về bảo mật kỹ thuật số trong nội bộ. Họ có xu hướng tìm kiếm ít thông tin hơn từ các nguồn bên ngoài về bảo mật kỹ thuật số và không áp dụng các quy trình chính thức để phát hiện các hành vi xâm nhập. Bên cạnh đó, doanh nghiệp cũng thường ít cập nhật các thủ tục và đầu tư ít vào bảo mật kỹ thuật số.

Vì vậy, các quốc gia đặt mục tiêu khuyến khích DNVVN áp dụng các phương thức tăng cường bảo mật kỹ thuật số hiệu quả hơn thông qua các chương trình chứng nhận, tiêu chuẩn bảo mật hoặc bằng cách nâng cao nhận thức và xây dựng năng lực bảo mật kỹ thuật số cho doanh nghiệp. Các sáng kiến chính sách thường không dành riêng cho DNVVN hoặc không được thiết kế đặc biệt cho loại hình doanh nghiệp này, mặc dù các xu hướng chính sách gần đây cho thấy sự thay đổi theo hướng tiếp cận có mục tiêu.

*Biên soạn: Trung tâm Thông tin và Thống kê Khoa học và Công nghệ*

## TÀI LIỆU THAM KHẢO CHÍNH

1. Andrews, D., G. Nicoletti and C. Timiliotis (2018), “*Going digital: What determines technology diffusion among firms?*”, [https://one.oecd.org/document/ECO/CPE/WP1\(2018\)8/en/pdf](https://one.oecd.org/document/ECO/CPE/WP1(2018)8/en/pdf) (aĐTĐMessed on 16 July 2018).
2. Eurostat (2020), *The Digital Economy and Society Index (DESI)*, <https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi> (aĐTĐMessed on 29 November 2020).
3. European Commission (2020), *Supporting Specialised Skill Development: Big Data, Internet of Things and Cyber Security for SMEs – Final report*, <https://op.europa.eu/en/publication-detail/-/publication/bb5c6c09-6285-11ea-b735-01aa75ed71a1/language-en>.
4. OECD (2021), *The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship*, OECD Publishing, Paris, <https://doi.org/10.1787/bdb9256a-en>.
5. OECD (2020), *OECD Digital for SMEs Global Initiative*, <https://www.oecd.org/going-digital/sme/> (aĐTĐMessed on 29 November 2020).
6. OECD (2019), *OECD SME and Entrepreneurship Outlook 2019*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/34907e9c-en>.
7. OECD (2020), “*Coronavirus (COVID-19): SME policy responses*”, *OECD Policy Responses to Coronavirus (COVID-19)*, <http://www.oecd.org/coronavirus/policy-responses/coronavirus-covid-19-sme-policy-responses-04440101/> (aĐTĐMessed on 18 July 2020).
8. OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, <https://doi.org/10.1787/bb167041-en>.