Đảm bảo an ninh mạng - Nền tảng quan trọng để phát triển thương mại điện tử

PGS. TS. HOÀNG THỊ THANH NHÀN
Trường Đại học Đông Đô

● NGÀY NHẬN BÀI: 13/9/2022 ● NGÀY GỬI PHẢN BIỆN: 18/9/2022
● NGÀY DUYỆT ĐĂNG: 04/10/2022

Tóm tắt: Trải qua hơn ba thập kỷ phát triển, thương mại điện tử (TMĐT) toàn cầu đã có những bước tiến đáng kể, đặc biệt kể từ khi đại dịch COVID-19 bùng nổ. Bên cạnh những thành công, sự phát triển của TMĐT còn tồn tại một số vấn đề lớn cần được giải quyết, liên quan đến an ninh, an toàn và bảo vệ quyền riêng tư cho khách hàng cũng như doanh nghiệp, về lòng tin của người tiêu dùng và về một số loại phí có thể phát sinh làm tăng giá hàng hóa, dịch vụ. Bài viết tập trung làm rõ khái niệm và nội dung an ninh trong TMĐT cũng như các giải pháp đảm bảo an ninh trong lĩnh vực hoạt động này dưới góc độ lý luận và thực tiễn thế giới.

Từ khóa: An ninh mạng, đảm bảo an ninh mạng, không gian mạng, thương mại điện tử.

1. AN NINH TRONG THƯƠNG MẠI ĐIỆN TỬ

Thương mại điện tử là hoạt động trao đổi hàng hóa và dịch vụ giữa các bên thông qua mạng Internet, tức là qua không gian mạng với sự tham gia của bên thứ ba có liên quan như ngân hàng, tổ chức tài chính, đơn vị vận chuyển/logistics. Trong không gian đó, có khá nhiều rủi ro có thể xảy ra cho các bên tham gia và cho chính không gian mạng. Với người tiêu dùng/mua hàng, rủi ro có thể là bị mất thông tin cá nhân, tài chính, bị gian lận trong thanh toán, tiếp cận các website giả mạo,... Với người bán hàng và các bên liên quan khác, rủi ro có thể là bị đánh cắp thông tin khách hàng, giao dịch, tài chính, mất lòng tin của khách hàng, làm giảm uy tín của công ty,... Những rủi ro trên đều bắt nguồn từ sự mất an toàn trong không gian mạng được tạo ra bởi nhiều công cụ tấn công khác nhau, như tấn công theo hình thức lừa đảo, giả mạo (spam, phishing), bằng chương trình đánh cắp thông tin tự động (Bots), từ chối thực hiện dịch vụ (DoS, DDoS), tấn công các websites TMĐT bằng các chương trình như Brute-force attack, SQL injections, tấn công mạng máy tính qua Trojan Horse, các virus, tấn công chéo (XSS),... Đặc biệt, từ năm 2015, ghi nhận một hình thức tấn

công quy mô lớn với sự tham gia và kết nối của nhiều hacker ở các quốc gia khác nhau chủ yếu nhằm đánh cắp thông tin cá nhân và thẻ tín dụng của người dùng, được gọi là Magecart. Việc triển khai Magecart thường được bắt đầu bằng việc xâm nhập vào trang web với các tệp lệnh kiểu như Javascript code có nhiệm vụ lướt thông tin để sao chép và đánh cắp, thậm chí thay đổi nội dung trang web. Do vậy, nếu bị tấn công bởi Magecart thì thiệt hại đối với doanh nghiệp và các bên liên quan là rất lớn.

Ngày nay, khi hoạt động TMĐT qua thiết bị di động đang ngày càng phát triển, các smartphone cũng đang trở thành đối tượng bị tấn công khá mạnh, bởi hầu hết chúng đều không có phần mềm bảo vệ dữ liệu. Như vậy, nguy cơ mất an toàn, an ninh trong giao dịch điện tử bằng phương tiện này là khá cao. Sự tồn tại của các rủi ro đa dạng như vậy đã và đang tiếp tục là trở ngại lớn đối với sự phát triển của TMĐT, là mối quan tâm thường xuyên của cả bên bán và bên mua trong giao dịch điện tử. Hay nói cách khác, vấn đề an ninh và đảm bảo an ninh trong TMĐT có ý nghĩa rất quan trọng.

Giao dịch TMĐT được diễn ra theo một chu kỳ khép kín, bắt đầu bằng việc khách hàng tiếp cận thông tin trên các website bán hàng trực tuyến, lựa chọn, đặt hàng, rồi thông tin về đơn hàng được chuyển đến nhà sản xuất/người bán hàng, xử lý, giao hàng cho nhà vận chuyển và chuyển tới người mua hàng. Việc thanh toán diễn ra trực tuyến ngay khi đặt hàng hoặc trực tiếp khi nhận hàng, tùy theo từng giao dịch cụ thể. Yêu cầu đặt ra là toàn bộ quá trình giao dịch phải an toàn, bảo đảm an ninh thì giao dịch mới được coi là thành công.

NGÀY NAY, KHI HOẠT ĐỘNG TMĐT QUA THIẾT BỊ DI ĐỘNG ĐANG NGÀY CÀNG PHÁT TRIỂN, NGUY CƠ MẤT AN TOÀN, AN NINH TRONG GIAO DỊCH ĐIỆN TỬ BẰNG PHƯƠNG TIỆN NÀY LÀ KHÁ CAO.

Như vậy, an ninh trong TMĐT được hiểu là việc bảo vệ các tài sản điện tử, trước hết là thông tin, khỏi sự xâm nhập, sử dụng, làm thay đổi, phá hủy bất hợp pháp và nó là một phần của an ninh thông tin. Mục tiêu của an ninh thông tin trong TMĐT là nhằm bảo vệ tính bảo mật, bảo toàn tính toàn vẹn và đảm bảo tính sẵn có của dữ liệu.

Trong TMĐT, *bảo mật thông tin*, thường được hiểu như là quyền riêng tư, luôn là mục tiêu rất quan trọng. Nó đòi hỏi không chỉ không được tiết lộ thông tin trái phép, mà còn đảm bảo quyền tiếp cận của những người được phép và ngăn chặn khả năng tiếp cận của những người không được phép. Các công cụ chính phục vụ cho tiêu chí bảo mật, gồm mã hóa dữ liệu, kiểm soát quyền truy cập, xác thực nhiều cấp, cấp quyền truy cập và sử dụng tài nguyên dữ liệu và các công cụ bảo mật vật lý nhằm bảo vệ các tài sản điện tử khỏi các mối đe dọa vật lý như trộm cắp, phá hoại, hủy hoại và thiên tai. *Việc đảm bảo tính toàn vẹn* trong TMĐT là nhằm bảo vệ nguồn dữ liệu chính xác và tránh được sự sửa đổi trái phép, thông qua các công cụ như sao lưu, tổng kiểm tra, mã chỉnh dữ liệu. Trong TMĐT, *việc đảm bảo tính sẵn có* của thông tin bất cứ khi nào cần đến là vô cùng quan trọng. Do đó, chúng cần được lưu trữ trong các khu vực an toàn

và luôn có các thiết bị dự phòng để ứng phó với bất cứ rủi ro nào có thể xảy ra.

2. CÁC GIẢI PHÁP ĐẢM BẢO AN NINH TRONG THƯƠNG MẠI ĐIỆN TỬ

Xuất phát từ tầm quan trọng vấn đề an ninh đối với sự phát triển của TMĐT, các chuyên gia cho rằng cần phải xây dựng chiến lược đảm bảo an ninh nhằm đạt được hai mục đích chính: Bảo vệ tính toàn vẹn của mạng lưới kinh doanh và các hệ thống nội bộ của nó; và đảm bảo giao dịch an toàn giữa khách hàng và cơ sở kinh doanh. Các nội dung chính, gồm đảm bảo an ninh giao dịch, quyền riêng tư, an ninh hệ thống và nhận thức, ứng phó với tội phạm mạng. Để đảm bảo an ninh trong TMĐT, nhiều giải pháp khác nhau đã được áp dụng. Có thể phân chia chúng thành *3 nhóm cơ bản* sau đây:

- *Nhóm giải pháp đảm bảo an ninh mạng cho cả hệ thống và cho từng ứng dụng*, gồm giải pháp chống xâm nhập và tấn công từ chối dịch vụ thông qua ứng dụng các công nghệ phát hiện, công nghệ thống kê phân tích để phát hiện các mối nguy cơ, giải pháp tường lửa, mã hóa, giải pháp bảo vệ máy trạm và người dùng cuối.

- *Nhóm giải pháp cho các nhà cung cấp hàng hóa và dịch vụ*, bao gồm sử dụng các giao thức HTTPS nhằm bảo mật thông điệp truyền tải giữa các máy chủ và khách hàng, bảo mật máy chủ và áp dụng các nguyên tắc an toàn trong quản trị website, như đặt mật khẩu khó, thay đổi định kỳ, kiểm soát phần mềm lạ, không tin cậy, phân quyền tài khoản và cảnh báo nguy cơ, áp dụng bảo mật nhiều tầng, bảo mật hệ thống thanh toán thông qua tích hợp chứng chỉ SSL (secure socket layer) mã hóa thông tin

> **AN NINH TRONG TMĐT ĐƯỢC HIỂU LÀ VIỆC BẢO VỆ CÁC TÀI SẢN ĐIỆN TỬ, TRƯỚC HẾT LÀ THÔNG TIN, KHỎI SỰ XÂM NHẬP, SỬ DỤNG, LÀM THAY ĐỔI, PHÁ HỦY BẤT HỢP PHÁP VÀ NÓ LÀ MỘT PHẦN CỦA AN NINH THÔNG TIN.**

truyền tải, xác nhận nhiều cấp, lưu biểu tượng của người dùng mà không lưu thông tin thẻ tín dụng của họ, tạo cổng thanh toán riêng và giải pháp sao lưu dữ liệu, nâng cao nhận thức bảo mật cho nhân viên.

- *Nhóm giải pháp cho khách hàng/người tiêu dùng*, gồm lựa chọn nền tảng TMĐT có uy tín, sử dụng phần mềm diệt virus, nâng cao nhận thức về tấn công mạng và cách phòng, chống.

Nhìn chung, các giải pháp rất đa dạng và việc lựa chọn chúng là tùy thuộc vào vai trò của các bên tham gia và hoàn cảnh cụ thể khi vụ việc diễn ra. Điều quan trọng cần ghi nhận là tất cả các bên tham gia đều phải quan tâm và thực hiện một cách phù hợp và kịp thời các chương trình, kế hoạch đảm bảo an toàn ngay từ khi bắt đầu bất cứ hoạt động thương mại nào trong không gian mạng.

3. CÁC HOẠT ĐỘNG TẤN CÔNG THƯỜNG GẶP TRONG THƯƠNG MẠI ĐIỆN TỬ

Các cuộc tấn công mạng nói chung và tấn công hoạt động TMĐT nói riêng diễn ra liên tục, ngày càng tinh vi hơn, với tần suất khác nhau, được thể hiện thông qua một số đặc điểm sau:

- Gia tăng số lượng người tham gia vào hoạt động TMĐT và gia tăng khối lượng

Bảng 1: Các hình thức tấn công mạng 2019 - 2020 (% trên tổng số)

Lĩnh vực	XSS[1]	SSRF[2]	SQLi	Spam	RCE/ RFI[3]	Path traversal[4]	Tải tệp tin	Rò rỉ dữ liệu	Trojan	Bỏ qua xác thực
Toàn nền kinh tế	14,5	0,7	10,9	3,3	23,9	12,6	9,0	17,9	6,1	1,0
Bán lẻ	16,3	0,6	12,8	2,1	21,0	11,3	8,3	21,0	5,9	0,6

Nguồn: IMPERVA (2020), p. 6

giao dịch trực tuyến luôn hấp dẫn các tin tặc trên không gian mạng, làm cho *số lượng các cuộc tấn công* mạng cũng gia tăng. Theo số liệu của IMPERVA (2020), mỗi tuần có hàng trăm vụ tấn công mạng trong lĩnh vực bán lẻ trên thế giới.

- *Hình thức tấn công* luôn đa dạng và có sự khác nhau không quá lớn giữa ngành bán lẻ và của toàn bộ nền kinh tế (bảng 1). Đáng ghi nhận là có sự gia tăng ở tất cả các hình thức tấn công mạng trong lĩnh vực TMĐT vào mùa mua sắm năm 2020 so với năm 2019. Cụ thể, tấn công Bots tăng 32%, DdoS: 38%, lướt thẻ tín dụng: 43%, gian lận thẻ tín dụng: 65%, tấn công bằng chương trình SQL Injection: 45%, đánh cắp tài khoản: 41%, Magecart: 81% và số lượng các websites bị tấn công tăng 53% (WEBSCALE (2021), p.3). Số liệu thống kê cho thấy Magecart đang là một "dịch bệnh" thật sự trong hoạt động tấn công mạng và mục đích chính là nhằm chiếm đoạt các thông tin cá nhân và tài chính của cả bên bán và bên mua trong TMĐT, gây thiệt hại về tài chính và uy tín của họ.

"CHIẾN LƯỢC ĐẢM BẢO AN NINH NHẰM ĐẠT ĐƯỢC HAI MỤC ĐÍCH CHÍNH: BẢO VỆ TÍNH TOÀN VẸN CỦA MẠNG LƯỚI KINH DOANH VÀ CÁC HỆ THỐNG NỘI BỘ CỦA NÓ; VÀ ĐẢM BẢO GIAO DỊCH AN TOÀN GIỮA KHÁCH HÀNG VÀ CƠ SỞ KINH DOANH."

- *Về nguồn gốc và phân bổ các cuộc tấn công mạng*: Các cuộc tấn công mạng trong ngành bán lẻ, bao gồm cả TMĐT, phần lớn có nguồn gốc nặc danh, chiếm tới 36,24%, trong khi với toàn bộ nền kinh tế, tỷ lệ này chỉ là 4,2% trong tổng số các vụ tấn công (IMPERVA (2020), p.7). Địa điểm khởi nguồn các cuộc tấn công mạng nhiều nhất trong lĩnh vực bán lẻ/TMĐT là nước Nga, chiếm tới 76% số cuộc tấn công khởi phát trong thời gian từ tháng 10/2019 đến tháng 9/2020, trong khi số vụ tấn công nhằm vào nước này chỉ chiếm 14,6%. Tiếp sau Nga là Tây Ban Nha với 8,85% và Mỹ với 8,54% số vụ khởi phát (IMPERVA (2020), p.11). Đích đến của các cuộc tấn công mạng trong ngành bán lẻ/TMĐT chủ yếu nhằm vào các website hoạt động trên thị trường Mỹ, tới 49% tổng các cuộc tấn công toàn cầu trong thời gian từ tháng 10/2019 đến tháng 9/2020. Trong khi đó, ba thị trường tiếp sau Mỹ, số vụ tấn công trong thời gian trên chỉ chiếm tương ứng 9% ở Pháp, 8% ở Anh và 7% ở Brazil. Đặc biệt, số vụ tấn công mạng vào các website ở Trung Quốc lại chủ yếu ở các ngành công nghiệp khác, hầu như không có trong ngành bán lẻ/TMĐT (IMPERVA (2020), p. 8).

- Bots, thường được sử dụng để chạy tự động và liên tục các thao tác nhất định - *đang vận hành hầu hết các cuộc tấn công mạng*. Hay nói theo ngôn ngữ đơn giản hơn, rất nhiều hoạt động tấn công mạng liên quan đến thu thập thông tin đều thực hiện tự động. Do đó, nguy cơ mất an toàn thông tin ở đây là rất lớn.

- Các cuộc tấn công thông qua các *chương trình độc hại để đánh cắp thông tin* thẻ tín dụng, thanh toán,... trên điện thoại thông minh đang có xu hướng gia tăng, khi TMĐT qua thiết bị di động đang tăng lên (nửa đầu năm 2019 tăng 50% số vụ so với cùng kỳ năm 2018).

- Có sự *chuyển hướng sang tấn công vào các chuỗi cung ứng và gia tăng tấn công vào đám mây công cộng*, nơi lưu giữ thông tin của các doanh nghiệp và phục vụ cho hoạt động làm việc từ xa và không dây. Và đó cũng chính là lý do để tin tặc có sự chuyển hướng này.

Trước sự gia tăng của số lượng, tần suất, cũng như sự đa dạng của các hình thức tấn công mạng trong các hoạt động của đời sống kinh tế xã hội nói chung và trong lĩnh vực bán lẻ nói riêng, đặc biệt từ khi bùng nổ đại dịch COVID-19, thực trạng an ninh TMĐT đang có chiều hướng bị xấu đi, làm gia tăng tính dễ bị tổn thương. Chỉ tính riêng trong năm 2020 đã có nhiều vụ tấn công xảy ra trong lĩnh vực TMĐT, làm lộ thông tin cá nhân khách hàng, thông tin hoạt động được lưu trữ nhiều năm của doanh nghiệp. Đối tượng bị các hacker nhắm tới không chỉ là các doanh nghiệp vừa và nhỏ với trang thiết bị bảo mật hạn chế mà cả nhiều doanh nghiệp lớn, có phạm vi hoạt động toàn cầu, với nhiều cơ sở, chi nhánh ở nhiều nước khác nhau, với hàng triệu khách hàng hiện hữu và tiềm năng. Ví dụ như vụ tấn công vào tập đoàn Travelex, chuyên cung cấp dịch vụ tiền tệ và du lịch toàn cầu vào tháng 1/2020, đã gây ảnh hưởng đến hoạt động của 1.200 cơ sở của tập đoàn này tại 70 nước trên thế giới và rất nhiều bên liên quan khác, trước hết là các ngân hàng. Hay như vụ tấn công vào Tập đoàn khách sạn Mariott cũng trong tháng 1/2020, chỉ thông qua việc đánh cắp được thông tin truy cập vào hệ thống của 2 nhân viên mà thông tin tài khoản và bảo mật của 5,2 triệu khách hàng đã bị đánh cắp. Vụ tấn công vào công ty game Nintendo của Nhật Bản trong tháng 4 và 6/2021 đã làm cho dữ liệu của 300.000 khách hàng bị đánh cắp.

Dựa trên những thông tin trong các báo cáo về thực trạng an ninh TMĐT những năm gần đây, có thể chỉ ra một số xu hướng cơ bản như sau:

- Các cuộc tấn công Magecart xảy ra ngày càng liên tục, do đó, nó được gọi là đại dịch thứ hai đe dọa an ninh của TMĐT toàn cầu. Trong năm 2020, 13 nhóm tội phạm mạng khác nhau đã gây ra trên 2,5 triệu vụ xâm nhập dưới dạng lướt thông tin đối với khoảng trên 25.000 website trên toàn cầu. Để ngăn chặn các vụ tấn công lướt mạng kiểu này, có thể áp dụng biện pháp mã kiểm tra kỹ lưỡng, chính sách đảm bảo an ninh nội dung để tránh sự xâm nhập

"CÁC CUỘC TẤN CÔNG MẠNG NÓI CHUNG VÀ TẤN CÔNG HOẠT ĐỘNG TMĐT NÓI RIÊNG DIỄN RA LIÊN TỤC, NGÀY CÀNG TINH VI HƠN, VỚI TẦN SUẤT KHÁC NHAU."

của các tệp lạ, xác nhận nhiều tầng và quét mã độc ngoại vi để loại trừ nó ngay từ vòng ngoài.

- Số lượng các Bots đánh cắp tài khoản trong TMĐT lớn gấp 2 lần so với các ngành khác. Theo số liệu của IMPERVA, năm 2020, số lượng tài khoản bị đánh cắp khi đăng nhập trong lĩnh vực TMĐT là 62%, trong khi ở các ngành khác chỉ là 25%.

- Kỹ thuật tấn công ngày càng tinh vi hơn. Các hacker có thể lấy cắp thông tin trước khi chúng được mã hóa. Thực tế này đòi hỏi phải duy trì việc sao lưu thông tin trực tiếp, có chiến lược ngăn chặn việc đánh cắp thông tin và nâng cao nhận thức của người dùng/khách hàng.

4. ĐẢM BẢO AN NINH MẠNG - NỀN TẢNG CỦA AN NINH TRONG THƯƠNG MẠI ĐIỆN TỬ

Do hoạt động tấn công mạng xảy ra thường xuyên, ngày càng gia tăng về tần suất và quy mô, nên khi tham gia TMĐT, các nước đều rất quan tâm đến việc hoàn thiện chiến lược, chính sách, biện pháp và năng lực thực thi nhằm đảm bảo an ninh, an toàn trong TMĐT. Thậm chí, theo WEBSCALE (2021), năm 2020, đầu tư cho IT giảm đi, song đầu tư cho quản trị rủi ro và an ninh mạng thì lại tăng lên.

Kết quả của những nỗ lực của các bên liên quan trong việc đảm bảo an ninh mạng nói chung và an ninh TMĐT nói riêng được thể hiện qua Chỉ số An ninh mạng Toàn cầu (Global Cybersecurity Index GCI). Đây là chỉ số tổng hợp dùng để đo mức độ thực hiện cam kết của các nước tham gia Chương trình An ninh mạng Toàn cầu (Global Cybersecurity Agenda GCA) được Liên minh Viễn thông quốc tế (International Telecommunication Union ITU) thông qua năm 2007. Các cam kết theo GCA có 5 nhóm, gồm luật pháp, kỹ thuật, tổ chức, xây dựng năng lực và hợp tác nhằm các mục tiêu: Hoàn thiện khung khổ pháp lý điều chỉnh hoạt động phòng chống tội phạm trên không gian mạng; đáp ứng những đòi hỏi về kỹ thuật, tiêu chuẩn, kỹ năng để bảo vệ và phản ứng trước các cuộc tấn công mạng; xây dựng và thực hiện hiệu quả chiến lược quốc gia, các cơ quan chịu trách nhiệm chính và hệ thống các giải pháp đảm bảo an ninh mạng; phát triển năng lực không chỉ cho lực lượng chuyên môn, kỹ thuật cao cho phòng chống tội phạm mạng mà cả nhận thức của cộng đồng và các bên liên quan khác; tham gia và phối hợp hiệu quả giữa các bên liên quan và hợp tác quốc tế trong đảm bảo an ninh mạng toàn cầu.

Cuộc khảo sát đầu tiên về GCI được thực hiện vào năm 2013 - 2014 và báo cáo đầu tiên được phát hành vào năm 2015 với sự tham gia của 105 nước trong tổng số 193 nước thuộc ITU, chiếm 54%. Sau đó, số lượng tham gia tăng dần, năm 2017 là 69%, năm 2018 khoảng 80% và năm 2020 là 87%, thể hiện sự quan tâm của các nước vào việc đảm bảo an ninh mạng theo cam kết quốc tế GCA. Những số liệu ở Bảng 2

> **TRƯỚC SỰ GIA TĂNG CỦA SỐ LƯỢNG, TẦN SUẤT, CŨNG NHƯ SỰ ĐA DẠNG CỦA CÁC HÌNH THỨC TẤN CÔNG MẠNG, AN NINH TMĐT ĐANG CÓ CHIỀU HƯỚNG BỊ XẤU ĐI, LÀM GIA TĂNG TÍNH DỄ BỊ TỔN THƯƠNG.**

Bảng 2: Top 10 nước đứng đầu bảng xếp hạng GCI 2018 và 2020 và Việt Nam

2018			2020		
Nước	**Giá trị**	**Xếp hạng**	**Nước**	**Giá trị**	**Xếp hạng**
Anh	0,931	1	Mỹ	100	1
Mỹ	0,926	2	Anh	99,54	2
Pháp	0,918	3	Saudi Arabia	99,54	2
Lithuania	0,908	4	Estonia	99,48	3
Estonia	0,905	5	Hàn Quốc	98,52	4
Singapore	0,898	6	Singapore	98,52	4
Tây Ban Nha	0,896	7	Tây Ban Nha	98,52	4
Malayxia	0,893	8	Nga	98,06	5
Canada	0,892	9	Tiểu vương quốc Arap thống nhất	98,06	5
Na-uy	0,892	10	Malayxia	98,06	5
			Lituania	97,93	6
			Nhật Bản	97,82	7
			Canada	97,67	8
			Pháp	97,6	9
			Ấn Độ	97,5	10
Việt Nam	0,693	50	Việt Nam	94,59	25

Nguồn: Global Cybersecurity Index 2018, p. 62 & Global Cybersecurity Index 2020, p. 25.

cho thấy những nước trong top 10 về GCI hầu như đã cam kết thực hiện đầy đủ các yêu cầu của GCA và Việt Nam đã có được bước tiến rất ấn tượng khi tăng được 25 bậc giữa hai lần xếp hạng các năm 2018 và 2020.

Thông qua các báo cáo về GCI, có thể đưa ra một số nhận xét sau:

- Sự chênh lệch giữa những nước đứng trong top 10 và 10 nước cuối bảng là rất lớn, giá trị tương ứng năm 2018 là 0,931 - 0,892 và 0,044 - 0,004; năm 2020 là 100 - 94,59 và 4,2 - 0,0. Tính không đồng đều này xảy ra cả ở cấp khu vực.

- Trong 5 lĩnh vực cam kết, cam kết ở lĩnh vực luật pháp và tổ chức là ở mức cao nhất và số lượng các nước tham gia nhiều nhất ngay từ khi GCI bắt đầu được thực hiện. Có nước ban hành Luật An ninh mạng (Lithuania, Singapore), Luật An ninh thông tin (Serbia), Luật An ninh quốc gia (Tây Ban Nha); có nước xây dựng các kế hoạch và chương trình hành động số (Bỉ, Moldova); có nước hoàn thiện luật pháp theo hướng tăng cường hợp tác quốc tế (Anh) hay trên cơ sở tăng cường nền tảng kỹ thuật (Nhật Bản với IoT). Đặc biệt, ngày càng có nhiều nước đưa ra các quy định về bảo vệ trẻ em

Bảng 3: Kết quả các cam kết theo GCI của các nước ITU đến hết năm 2020

Văn bản pháp luật	Số nước đã phê chuẩn/ thực hiện	Số nước đang soạn thảo/chuẩn bị	Số nước chưa thực hiện
Về luật pháp			
Luật/qui định về bảo vệ dữ liệu	133	15	49
Các biện pháp thông báo vi phạm	102	4	88
Luật/qui định điều chỉnh về ăn cắp thông tin cá nhân	97	17	80
Qui định về xâm nhập bất hợp pháp	157	9	28
Luật/qui định về các hành vi phản xã hội trực tuyến	100	17	77
Qui định về bảo vệ trẻ em trên không gian mạng	27	59	108
Về kỹ thuật			
Đội phản ứng nhanh quốc gia	131	5	58
Đội phản ứng nhanh của một số ngành đặc trưng	84	-	109
Về tổ chức			
Chiến lược an ninh mạng quốc gia	119	6	70
Đánh giá chiến lược an ninh mạng quốc gia	Có: 60	Một phần: 5	Không: 129
Kiểm soát an ninh mạng cấp quốc gia	Có: 88	Một phần: 1	Không: 105
Thước đo để đánh giá rủi ro trong không gian mạng ở cấp quốc gia	Có: 74	Một phần: 2	Không có: 118
Về xây dựng năng lực			
Chiến dịch nâng cao nhận thức cho SMEs, khu vực tư nhân và các cơ quan chính phủ	Có: 116	Một vài: 3	Không có: 75
Thực hiện các chương trình đào tạo	90	2	102
Cơ chế khuyến khích phát triển năng lực an ninh mạng	Có: 70	-	Không: 124
Về hợp tác			
Tham gia hiệp định song phương	Có: 123	Chuẩn bị: 5	Chưa: 99
Đã ký và phê chuẩn hiệp định đa phương	Có: 112	Chuẩn bị: 2	Chưa: 80
Tham gia vào các hoạt động quốc tế	140	-	54
Hợp tác công tư trong nước hoặc quốc tế	Trong nước:63 Quốc tế: 13		104

Nguồn: ITU (2021), p. 3-23.

trên không gian mạng. Về cơ bản, hệ thống luật pháp liên quan đến điều chỉnh hoạt động trên không gian mạng là khá đầy đủ (Bảng 3).

- Dưới góc độ tổ chức, phần lớn các nước đã xây dựng chiến lược đảm bảo an ninh mạng, cơ chế tổ chức thực hiện và các giải pháp liên quan, trong đó nhấn mạnh việc phối hợp giữa các cơ quan liên quan trong nước và quốc tế, xây dựng các trung tâm chia sẻ thông tin, phát triển cơ sở hạ tầng thông tin, đặc biệt là vấn đề bảo mật. Nhiều nước đã thành lập Trung tâm an ninh mạng quốc gia (Singapore, Cô-oét), hay Trung tâm quốc gia về sẵn sàng ứng phó và chiến lược an ninh mạng (Nhật Bản); có cơ chế đánh giá chiến lược định kỳ nhằm có những điều chỉnh, bổ sung cho phù hợp. Chiến lược an ninh mạng quốc gia hướng tới việc bảo vệ cơ sở hạ tầng và nâng cao năng lực phòng chống tội phạm mạng. Nhiều nước còn kết hợp giữa thực hiện chiến lược với tăng cường hiệu quả hoạt động của các đội phản ứng nhanh nhằm gia tăng độ an toàn trên không gian mạng. Nhờ đó, tỷ lệ người dân sử dụng Internet được bảo vệ là khá cao, có thể lên tới 95%. Trong khi đó, ở những nước chưa có chiến lược và đội phản ứng nhanh, tỷ lệ này chỉ đạt 15% (ITU (2021), p. 11).

- Ba lĩnh vực còn lại của GCI gồm kỹ thuật, xây dựng năng lực và hợp tác, bao gồm cả hợp tác quốc tế thường có mức độ cam kết thấp hơn, đặc biệt là ở các nước đang phát triển có thu nhập trung bình trở xuống và nằm ở các vị trí địa lý kém thuận lợi và do đó, thứ hạng của họ trong bảng xếp hạng GCI toàn cầu cũng thấp hơn.

Các cam kết về kỹ thuật gồm thành lập các đội phản ứng nhanh với tấn công mạng, áp dụng tiêu chuẩn về an ninh mạng, xây dựng cơ chế kỹ thuật và năng lực phát hiện thư rác, năng lực sử dụng đám mây và các biện pháp bảo vệ trẻ em trên không gian mạng. Đây là những cam kết đòi hỏi phải có nguồn nhân lực phù hợp khi thực hiện. Cam kết về xây dựng năng lực rất đa dạng, bao gồm nâng cao năng lực an ninh mạng trong các ngành kinh tế, thúc đẩy R&D, thực hiện các chương trình giáo dục phổ cập và chuyên ngành về an ninh mạng và các sáng kiến cộng đồng nhằm nâng cao nhận thức về an ninh mạng. Về hợp tác, nhất là hợp tác quốc tế, thì hạn chế nhất vẫn là một số nước châu Phi. Thực tế tốt hơn nhiều với các nước châu Âu, tiếp đến là châu Mỹ và châu Á - Thái Bình Dương.

> **CÁC CAM KẾT THEO GCA CÓ 5 NHÓM, GỒM LUẬT PHÁP, KỸ THUẬT, TỔ CHỨC, XÂY DỰNG NĂNG LỰC VÀ HỢP TÁC.**

- Thực tế cho thấy các nước có GCI cao hơn, thường cũng đạt được thứ hạng cao trong các bảng xếp hạng khác về Chỉ số Phát triển Chính phủ điện tử, Chỉ số Phát triển ICT. Do đó, sẽ hỗ trợ nhiều cho việc đảm bảo an ninh khi tham gia hoạt động trên không gian mạng.

5. CÁC BIỆN PHÁP ĐẢM BẢO AN NINH TRONG THƯƠNG MẠI ĐIỆN TỬ

5.1. Về luật pháp

Theo thống kê của UNCTAD, cho đến nay, 81% số nước trên thế giới đã ban hành Luật giao dịch TMĐT (đa số các nước châu Phi và Trung Đông mới ban hành trong 3

năm gần đây), 59% số nước đã có Luật bảo vệ người tiêu dùng, 67% số nước có Luật về quyền riêng tư và 80% số nước đã ban hành Luật về tội phạm mạng. Như vậy, khung khổ pháp luật liên quan đến đảm bảo an ninh TMĐT ở nhiều nước đã được hoàn thiện. Đặc biệt, quyền lợi của người tiêu dùng, quyền riêng tư của các cá nhân tham gia giao dịch TMĐT, cũng như hoạt động ngăn ngừa và phòng chống tội phạm mạng đã và đang được quan tâm thích đáng. Căn cứ vào điều kiện cụ thể và quá trình phát triển hệ thống pháp luật của mình, mỗi nước sẽ cụ thể hóa những quy định cho phù hợp.

5.2. Về các biện pháp kỹ thuật để đảm bảo an ninh thương mại điện tử

Các nước đã và đang sử dụng nhiều biện pháp kỹ thuật khác nhau để đảm bảo an ninh trong TMĐT, tập trung chủ yếu vào bảo vệ thông tin cá nhân, thanh toán, như mã hóa đối xứng và không đối xứng, sử dụng chứng chỉ tích hợp SSL mã hóa thông tin truyền tải, áp dụng chuẩn bảo mật PCI DS, mật khẩu OPT, cơ chế lưu token của người dùng mà không lưu giữ thông tin thẻ, áp dụng thẻ thông minh, các kênh thanh toán có uy tín nội địa và quốc tế, tường lửa và các biện pháp chống xâm nhập khác nhau, sao lưu dữ liệu... Đặc biệt, nhiều nước đã quan tâm đến việc đào tạo không chỉ nhằm nâng cao ý thức của cộng đồng về an ninh và các biện pháp tự bảo vệ trong không gian mạng, mà cả các lao động làm việc trong lĩnh vực TMĐT và các lĩnh vực liên quan về trách nhiệm và nghĩa vụ của họ đối với việc bảo vệ thông tin cá nhân cho khách hàng, tính vẹn toàn và sẵn có của nó.

> **PHẦN LỚN CÁC NƯỚC ĐÃ XÂY DỰNG CHIẾN LƯỢC ĐẢM BẢO AN NINH MẠNG, CƠ CHẾ TỔ CHỨC THỰC HIỆN VÀ CÁC GIẢI PHÁP LIÊN QUAN, TRONG ĐÓ NHẤN MẠNH VIỆC PHỐI HỢP TRONG NƯỚC VÀ QUỐC TẾ, XÂY DỰNG CÁC TRUNG TÂM CHIA SẺ THÔNG TIN, PHÁT TRIỂN CƠ SỞ HẠ TẦNG THÔNG TIN, ĐẶC BIỆT LÀ VẤN ĐỀ BẢO MẬT.**

5.3. Đánh giá của người dùng về đảm bảo an ninh trong thương mại điện tử

Để minh chứng cho việc môi trường giao dịch TMĐT đã *đảm bảo an toàn về quyền riêng tư và thông tin cá nhân* hay chưa, có thể sử dụng kết quả điều tra quốc tế của Trung tâm Đổi mới Quản trị quốc tế của IPSOS kết hợp CIGI dưới sự hỗ trợ của UNCTAD và Internet Society, được thực hiện từ tháng 12/2018 đến hết tháng 2/2019 tại 25 quốc gia với trình độ phát triển khác nhau về TMĐT nói riêng và trình độ phát triển kinh tế nói chung. Sau đây là một số kết quả cụ thể:

- Tính trung bình, khoảng 48% dân số toàn cầu đồng ý rằng các chính phủ của họ đã đủ cố gắng trong việc bảo vệ thông tin cá nhân người dùng, cho dù dao động giữa các nước là khá lớn, từ khoảng 77% ở Indonexia xuống chỉ còn khoảng 27% ở Nhật Bản, các nước BRICS, châu Á - Thái Bình Dương, châu Phi, Mỹ La tinh có mức cao hơn trung bình của thế giới, trong khi các nước châu Âu, Bắc Mỹ, G8 thì thấp hơn.

- Trung bình khoảng 59% dân số toàn cầu đồng ý rằng các công ty mà họ có giao

dịch đã đủ cố gắng trong việc bảo vệ dữ liệu cá nhân, ngoại trừ Pháp và Nhật Bản chỉ có 37% đồng ý, còn Indonexia thì tới 82% đồng ý.

- Người dùng Internet đã có ý thức cao hơn trong việc tự bảo vệ mình khi tham gia không gian mạng bằng những biện pháp như tránh mở những email từ các địa chỉ lạ, không cung cấp nhiều thông tin cá nhân lên mạng, né tránh những website cảm thấy không an toàn, sử dụng phần mềm diệt virus, thay đổi mật khẩu thường xuyên, giảm thiểu các giao dịch tài chính và mua hàng trực tuyến, sử dụng Internet ít đi.

- Việc mua hàng hóa và dịch vụ trực tuyến đã dễ dàng hơn trước nhiều, tới 41% số người được hỏi cho rằng dễ dàng hơn năm trước, 51% cho rằng vẫn thế, chỉ 8% cho rằng khó khăn hơn, chủ yếu là ở châu Phi và Mỹ Latinh.

- Niềm tin của người sử dụng vào Internet có xu hướng gia tăng ở hầu hết các khu vực trên thế giới, với sự gia tăng mạnh hơn ở các nước đang phát triển so với nhóm các nước phát triển (IPSOS (2019), p.115). Những nước có tỷ lệ tin tưởng gia tăng nhiều nhất so với năm 2018 là Tunisia và Pakistan.

- Về các yếu tố tạo nên sự thiếu tin tưởng trên không gian mạng, đứng đầu danh sách là tội phạm mạng (với sự đồng ý của 81% số người được hỏi), tiếp đến là các công ty truyền thông (75%), các chính phủ nước ngoài và sở tại (66%), công cụ tìm kiếm (65%), các nhà cung cấp dịch vụ mạng (63%), các nền tảng TMĐT (61%), các nền tảng thanh toán trực tuyến và qua điện thoại thông minh (56%). Ngoài ra, còn một số nguyên nhân khác như vấn đề kiểm duyệt trên Internet, sự kiểm soát của các chính phủ và khó tìm được nội dung cần tìm kiếm.

Việc thanh toán trong trao đổi TMĐT toàn cầu được thực hiện thông qua nhiều phương thức khác nhau, như ví điện tử, thẻ tín dụng, thẻ ghi nợ, chuyển khoản qua ngân hàng, thanh toán tiền mặt khi nhận hàng, mua trả sau, thẻ trả trước, thanh toán qua bưu điện, trong đó 3 phương thức đầu phổ biến hơn cả. Trong bối cảnh thẻ tín dụng là đối tượng tấn công "hấp dẫn" đối với các tin tặc, nên các khách hàng và doanh nghiệp đều rất quan tâm đến việc đảm bảo an ninh thanh toán điện tử, nhất là khi nó được thực hiện qua thiết bị di động. Tuy nhiên, cho đến nay, đây vẫn còn là thách thức lớn. Kết quả từ một cuộc khảo sát của Pew cho thấy

THỰC TIỄN CHO THẤY, DÙ CÁC BÊN THAM GIA CÓ CỐ GẮNG ĐẾN ĐÂU THÌ VẪN PHẢI ĐỐI MẶT VỚI SỰ GIA TĂNG CỦA HOẠT ĐỘNG TẤN CÔNG MẠNG, BỞI CÔNG NGHỆ TẤN CÔNG CŨNG LUÔN ĐƯỢC HIỆN ĐẠI HÓA VÀ TRỞ NÊN TINH VI HƠN. NHÌN CHUNG, NHẬN THỨC VÀ MỨC ĐỘ ĐẢM BẢO AN NINH MẠNG ĐANG DẦN ĐƯỢC CẢI THIỆN Ở HẦU HẾT CÁC NƯỚC TRÊN THẾ GIỚI, KẾT HỢP VỚI NHỮNG CỐ GẮNG ĐẢM BẢO AN NINH TRONG TMĐT SẼ LÀ CƠ SỞ CHO VIỆC CẢI THIỆN MÔI TRƯỜNG TMĐT TRONG TƯƠNG LAI. BÊN CẠNH ĐÓ, VIỆC TỰ BẢO VỆ CỦA CÁC CÁ NHÂN KHI THAM GIA VÀO KHÔNG GIAN MẠNG TIẾP TỤC LÀ MỘT HƯỚNG ĐI QUAN TRỌNG TRONG VIỆC ĐẢM BẢO AN NINH CHO CHÍNH MÌNH TRÊN KHÔNG GIAN MẠNG.

tỷ lệ khách hàng lo lắng về mức bảo vệ kém trong thanh toán qua thiết bị di động là lớn nhất, tới 38% (Bảng 4). Trong nhiều trường hợp việc thông tin thanh toán không được bảo vệ ở mức cần thiết là một trong những nguyên nhân để khách hàng từ chối mua hàng trên các trang TMĐT.

Đảm bảo an ninh trong TMĐT hướng tới ba mục tiêu chính là bảo mật thông tin, tính toàn vẹn và sẵn có của nó; được thực hiện thông qua nhiều biện pháp khác nhau, kỹ thuật và phi kỹ thuật, từ các bên tham gia, gồm các chính phủ, các công ty TMĐT và cung cấp dịch vụ liên quan và các khách hàng/người tiêu dùng.

Bảng 4: Vấn đề an ninh thanh toán trong TMĐT (% trong tổng số người được hỏi)

Đánh giá	Thẻ tín dụng	Thẻ ghi nợ	Thẻ trả trước	Thanh toán qua thiết bị di động
Được bảo vệ ở mức kém	9	22	28	38
Được bảo vệ ở mức trung bình	28	34	35	38
Được bảo vệ tốt	61	43	34	22
(số còn lại là không trả lời hoặc không biết)				

Nguồn: https://ecommerceguide.com/guides/ecommerce-payment-stats-which-methods-do-shoppers-want/

TÀI LIỆU THAM KHẢO:

• Ansar Waseem, Yasir Rashid, Muhammad Akib Warraich, Imran Sadiq and Zeeshan Shaukat (2019), Factors Affecting E-commerce Potential of Any Country Using Multiple Regression Analysis, Journal of Internet Banking and Commerce, August 2019, vol. 24, no. 2, from http://www.icommercecentral.com.

• Deepak Kumar and Nivesh Goyal (2016), Security Issues in M-Commerce for Online Transaction, paper presented on the 5th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Sep. 7-9, 2016, AIIT, Amity University Uttar Pradesh, Noida, India.

• IMPERVA (2020), The State of Security within eCommerce Report, from imperva.com.

• IPSOS (2019), CIGI-IPSOS Global Survey Internet Security & Trust 2019, from https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey, part 1,2&6.

• ITU (2019), Global Cybersecurity Index 2018

• ITU (2021), Global Cybersecurity Index 2020 - Measuring commitment to cybersecurity.

• Kyung Han Sohn (2016), Privacy and Security Protection under Korean Ecommerce Law and Proposal for Its Improvements, Arizona Journal of International & Comparative Law Vol. 33, No. 1, p.229-248.

• N. Kuruwitaarachchi, P.K.W. Abeygunawardena, L.Rupasingha & S.W.I.Udara (2019), A Systematic Review of Security in Electronic Commerce- Threats and Frameworks, Global Journal of Computer Science and Technology: E Network, Web & Security, Volume 19 Issue 1 Version 1.0

• Randy C. Marchany and Joseph G. Tront (2002), E-commerce Security Issues from https://www.researchgate.net/publication/232643081

• WEBSCALE (2021), The Global Ecommerce Security Report 2021, published in February by Webscale Networks, Inc.