Rủi ro an ninh mạng trong hoạt động ngân hàng số: trường hợp Việt Nam

TS. Phan Chung Thủy TS. Phan Thu Hiền ThS. Huỳnh Ngọc Quang Anh

UEH University

RỦI RO AN NINH MẠNG TRONG HOẠT ĐỘNG NGÂN HÀNG SỐ: TRƯỜNG HỢP VIỆT NAM

TS. Phan Chung Thủy

Khoa Ngân Hàng, Đại học Kinh Tế TP. HCM

TS. Phan Thu Hiền

Khoa Ngân Hàng, Đại học Kinh Tế TP. HCM

ThS. Huỳnh Ngọc Quang Anh

Trung tâm Bồi dưỡng và Tư vấn Ngân hàng-Chứng khoán, Đại học Kinh Tế TP. HCM

TÓM TẮT

Rủi ro an ninh mạng là một trong những rủi ro quan trọng nhất trong lĩnh vực tài chính – ngân hàng. Trong thời đại công nghệ 4.0, các ngân hàng thương mại Việt Nam đã và đang trong quá trình chuyển đổi số, tiến đến mô hình ngân hàng số toàn diện trong tương lai. Ứng dụng công nghệ số mang lại nhiều cơ hội cho các ngân hàng nhưng cũng làm gia tăng nguy cơ về khả năng bị tấn công từ tội phạm mạng. Vì vậy, đảm bảo an toàn an ninh mạng là vấn đề sống còn của các ngân hàng Việt Nam trong tương lai.

Bài viết cung cấp một bức tranh toàn cảnh về rủi ro an ninh mạng và xu hướng phát triển ngân hàng số ở Việt Nam. Tiếp theo, chúng tôi đi sâu vào phân tích ảnh hưởng của rủi ro an ninh mạng đến hoạt động ngân hàng số cũng như những vấn đề còn tồn tại trong rủi ro và quản trị rủi ro an ninh mạng. Trên cơ sở đó, một số nhóm giải pháp được đề xuất để hạn chế rủi ro an ninh mạng: tập trung vào các nhân tố bao gồm quy trình, công nghệ và con người. Một số kiến nghị với Chính phủ và Ngân hàng Nhà nước cũng được chú trọng trong nghiên cứu này.

Từ khoá: *rủi ro an ninh mạng, ngân hàng số, công nghệ, tội phạm mạng, Việt Nam*

1. GIỚI THIỆU

Hiện nay, chuyển đổi số và ứng dụng công nghệ cao không phải là câu chuyện của riêng doanh nghiệp, mà còn của tất cả chúng ta. Tốc độ phát triển chóng mặt của công nghệ cũng như sự ảnh hưởng nặng nề của đại dịch Covid-19 đã khiến chúng ta nhận thức được sâu sắc tầm quan trọng của chuyển đổi số trong kỷ nguyên công nghệ 4.0. Bởi vì, những thứ cần thiết hàng ngày như chuỗi cung ứng thực phẩm, phương tiện vận chuyển, thanh

toán và giao dịch tài chính, hoạt động giáo dục, vận hành của chính phủ thậm chí cả khai thác nguồn tài nguyên như nước và năng lượng đang ngày càng phụ thuộc vào kỹ thuật và công nghệ số. Tuy nhiên, chính điều này làm cho chúng ta luôn có nguy cơ trở thành mục tiêu của các tội phạm mạng.

Cho nên chính sách an ninh mạng trở thành chính sách cốt lõi để bảo vệ quyền và lợi ích của mọi doanh nghiệp và người dân trong thời đại kỹ thuật số và đặc biệt là củng cố niềm tin của họ vào công nghệ kỹ thuật số. Thực tế cho thấy tội phạm mạng đang ngày càng gia tăng và thiệt hại do chúng gây ra ngày càng nghiêm trọng hơn. Theo báo cáo về an ninh mạng của IDP (2020), tội phạm mạng chiếm khoảng một nửa số tội phạm tài sản toàn cầu. Thiệt hại kinh tế do các cuộc tấn công mạng gây ra ước tính lên đến hơn 1% tổng sản phẩm quốc nội (GDP) hàng năm của các quốc gia, trong đó một số cuộc tấn công vào cơ sở hạ tầng quan trọng có thể gây ra thiệt hại đến 6% GDP hàng năm.

Trong các lĩnh vực bị tấn công, tài chính - ngân hàng là lĩnh vực thu hút sự chú ý nhất của tội phạm mạng. Trong báo cáo về tổn thất vi phạm dữ liệu trên phạm vi toàn thế giới do IBM (2020) thực hiện, chỉ tính riêng ngành dịch vụ tài chính đã thiệt hại 5.85 triệu USD do các tổn thất vi phạm dữ liệu. Trong số 17 ngành công nghiệp được IBM thực hiện khảo sát, ngành tài chính đứng thứ ba về chi phí tổn thất. Điều này xuất phát từ tính đặc thù của ngành tài chính ngân hàng bởi vì mô hình hoạt động kinh doanh cũng như việc cung ứng sản phẩm dịch vụ của ngành dựa trên nền tảng công nghệ kỹ thuật số.

Việt Nam hiện đứng thứ 21 trên thế giới về các vụ tấn công lừa đảo với 673,743 cuộc tấn công được ghi nhận trong năm 2020. Nếu xét riêng trong khu vực Đông Nam Á, Việt Nam đang trong nhóm dẫn đầu số vụ tấn công mạng chỉ sau Thái Lan và Indonesia. Còn theo báo cáo an ninh mạng Việt Nam của công ty Bkav, trung bình mỗi tháng, hệ thống giám sát virus của Bkav đã phát hiện hơn 15,000 phần mềm gián điệp trên điện thoại di động (Hồng Vinh, 2021). Còn theo báo cáo của Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao của Bộ Công an, các vụ tấn công an ninh mạng trong năm 2020 đã gây ra thiệt hại khoảng 100 tỷ đồng, trong đó có ngân hàng bị thiệt hại lên tới 44 tỷ đồng (Huyền Anh, 2020).

Trong thời gian qua, hệ thống ngân hàng thương mại Việt Nam đã tăng cường ứng dụng các công nghệ số hiện đại, nâng cao hiệu quả hoạt động, gia tăng trải nghiệm khách hàng và tạo thuận lợi cho khách hàng trong việc sử dụng dịch vụ ngân hàng hiện đại. Tuy nhiên, cùng với đó là những nguy cơ, lỗ hổng đã tạo điều kiện cho tội phạm mạng lợi dụng tiến hành các hành vi vi phạm pháp luật. Vì thế, bài nghiên cứu này nhằm mục

đích cung cấp bức tranh toàn diện về rủi ro an ninh mạng, xu hướng ngân hàng số và sự tác động của rủi ro an ninh mạng đến hoạt động ngân hàng số tại Việt Nam. Hơn nữa, bài viết cũng tập trung vào xây dựng các nhóm giải pháp cho quản trị rủi ro an ninh mạng tại ngân hàng số. Các nhóm giải pháp tập trung vào 3 yếu tố: quy trình quản trị, công nghệ và con người. Các kiến nghị đối với chính phủ và NHNN cũng được chú trọng. Điểm nổi bật là tất cả các kiến nghị và giải pháp của bài viết được xây dựng trên cơ sở phân tích các tồn tại và nguyên nhân trong vấn đề rủi ro an ninh mạng của hoạt động ngân hàng số Việt Nam.

2. KHÁI QUÁT VỀ RỦI RO AN NINH MẠNG

2.1. Khái niệm

Rủi ro mạng hay rủi ro an ninh mạng (cyber risk hay cybersecurity risk) là thuật ngữ được sử dụng để chỉ các rủi ro xảy ra từ quá trình hoạt động của công nghệ thông tin (CNTT) mà gây ảnh hưởng xấu đến tính bảo mật, tính sẵn có hoặc tính toàn vẹn của công nghệ hoặc hệ thống thông tin của tổ chức (Cebula và Young, 2010). Theo FSB (2018), rủi ro an ninh mạng là *"sự kết hợp của xác suất xảy ra sự cố mạng và sự tác động của chúng đến tổ chức"*. Trong đó, "sự cố mạng" là thuật ngữ để chỉ bất kỳ sự kiện nào xảy ra trong hệ thống thông tin mà (i) gây bất ổn cho hệ thống thông tin hoặc thông tin mà hệ thống đó xử lý, lưu trữ hoặc truyền đi; hoặc (ii) vi phạm các chính sách bảo mật, quy trình thủ tục đảm bảo an toàn hoặc chính sách sử dụng, cho dù là xuất phát từ hoạt động có gây hại hay không.

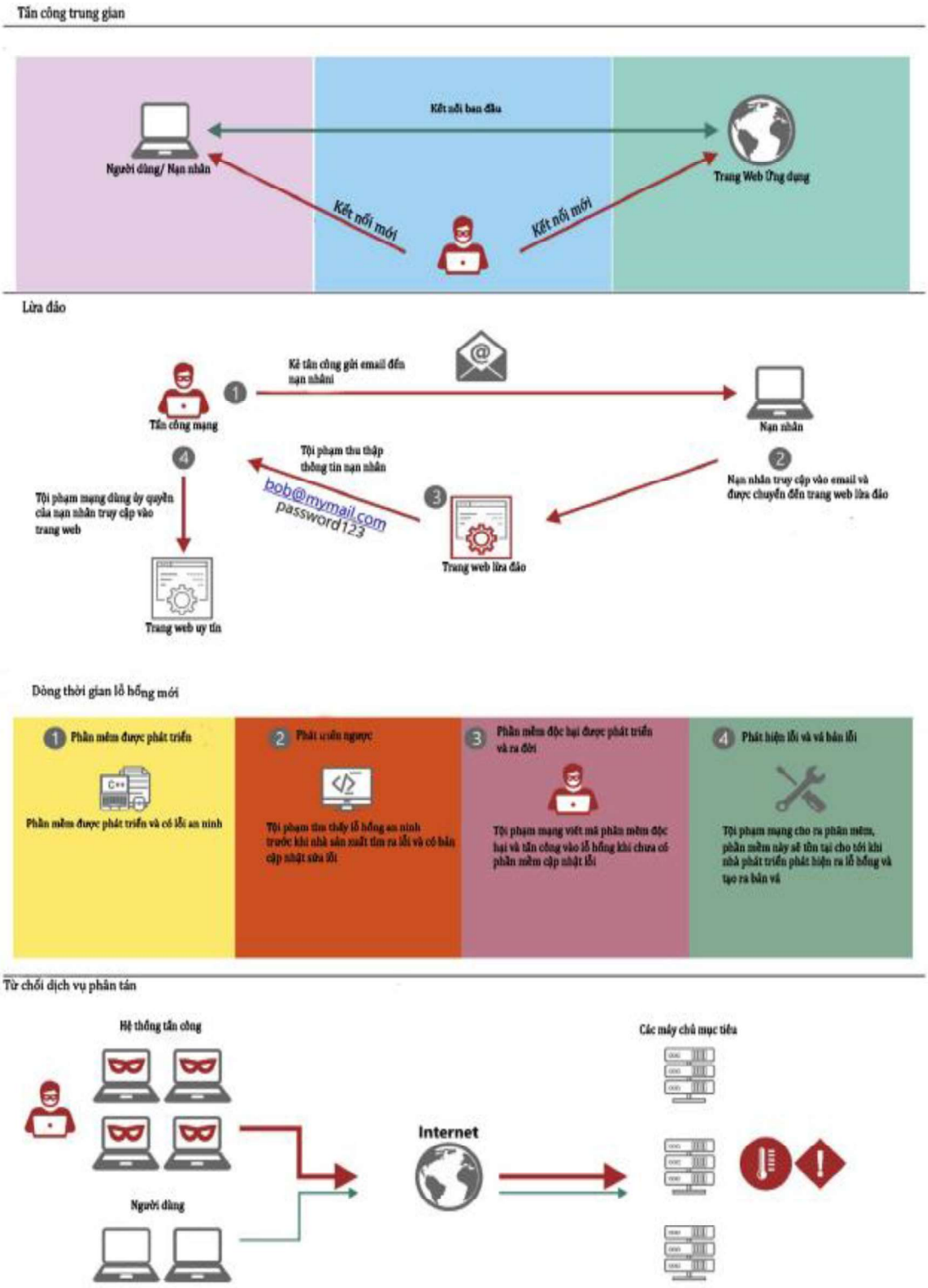
Theo cách giải thích đơn giản hơn, rủi ro an ninh mạng chính là nguy cơ mất mát hoặc thiệt hại do vi phạm hoặc tấn công vào hệ thống thông tin của một tổ chức. Hay nói cách khác, rủi ro an ninh mạng là *"khả năng mất mát hoặc tổn hại liên quan đến cơ sở hạ tầng kỹ thuật hoặc việc sử dụng công nghệ trong một tổ chức"* (RSA, 2016).

2.2. Phân loại

Hiện có 2 cách khác nhau để phân nhóm rủi ro an ninh mạng. Cách tiếp cận phổ biến đầu tiên dựa trên tính chất của các cuộc tấn công mạng (Cisco, 2020). Theo đó, có 7 loại phổ biến sau:

- Phần mềm độc hại (Malware): xảy ra khi tin tặc sử dụng các virus, sâu hay các loại phần mềm gián điệp để tấn công vào hệ thống thông tin của tổ chức. Tùy thuộc vào loại phần mềm độc hại, tin tặc sẽ (i) chặn quyền truy cập vào phần lõi của hệ thống; (ii) cài đặt thêm các phần mềm độc hại khác vào hệ thống; (iii) lấy cắp thông tin của ổ cứng; (iv) làm hỏng một số phần của hệ thống và cho nên hệ thống không thể hoạt động được.

- Tấn công trung gian (Man-in-the-middle, hay MitM): xảy ra khi tin tặc bí mật xen vào các giao dịch của hai bên, chẳng hạn như giữa người sử dụng máy tính cá nhân và tổ chức tài chính của họ. Sau đó, tin tặc có thể lấy cắp thông tin của người dùng. Hiện có hai dạng MitM phổ biến, bao gồm (i) ở các điểm wifi công cộng, kẻ gian có thể tự chèn vào giữa thiết bị của khách truy cập và mạng. Nếu không biết, người truy cập sẽ vô tình chuyển tất cả thông tin giao dịch cho kẻ gian; (ii) sau khi phần mềm độc hại xâm nhập vào thiết bị, kẻ gian có thể cài đặt phần mềm để tự ý xử lý tất cả thông tin của nạn nhân.
- Lừa đảo hoặc thực hiện câu nhử (Phishing): xảy ra khi tin tặc gửi các email để lôi kéo người nhận mở chúng. Người nhận bị lừa tải xuống máy tính cá nhân các phần mềm độc hại có trong email bằng cách mở tệp đính kèm hoặc liên kết được nhúng. Mục đích của tin tặc chính là ăn cắp dữ liệu của người dùng như thông tin thẻ tín dụng và thông tin đăng nhập.
- Dòng thời gian lỗ hổng mới hoặc khai thác lỗ hổng mới (Zero-day exploit): xảy ra sau khi lỗ hổng trong cơ sở hạ tầng CNTT của tổ chức được công bố nhưng trước khi tổ chức triển khai các biện pháp khắc phục.
- Từ chối dịch vụ phân tán (Distributed Denial-of-Services-DDoS): xảy ra khi tin tặc làm ngập hệ thống, máy chủ hoặc mạng, qua đó làm cho máy chủ và hệ thống của tổ chức không thể xử lý bất kỳ yêu cầu hợp pháp nào. Những kẻ tấn công cũng có thể sử dụng nhiều thiết bị bị xâm nhập của tổ chức để khởi động cuộc tấn công này.
- Tấn công máy chủ (Structure Query Language - SQL Injection): xảy ra khi tin tặc chèn mã độc vào máy chủ bằng ngôn ngữ truy vấn có cấu trúc (SQL); khi đó buộc máy chủ phải tiết lộ các thông tin nhạy cảm. Hình thức đơn giản nhất là kẻ gian có thể chèn mã SQL bằng cách gửi mã độc hại vào hộp tìm kiếm trên trang web của tổ chức.
- Đường hầm DNS (DNS Tunneling): xảy ra khi kẻ gian sử dụng cổng 53 của hệ thống để lấy dữ liệu khi hệ thống bị xâm nhập bằng các giao dịch DNS có cài mã độc. Bằng cách này, kẻ gian cũng có thể gọi lại các lệnh đã thực hiện trước đó và chiếm quyền điều khiển hệ thống.



Hình 1: Minh hoạ một số rủi ro an ninh mạng phổ biến

Nguồn: Aldasoro và cộng sự (2021)

Không giống như cách tiếp cận trên, cách tiếp cận thứ hai trong phân nhóm rủi ro an ninh mạng dựa trên nguyên nhân xảy ra của rủi ro an ninh mạng (RSA, 2016). Bởi vì theo quan điểm này, một rủi ro có thể là kết quả của các hành vi cố ý có hại, chẳng hạn như một tin tặc thực hiện một cuộc tấn công với mục đích lấy cắp những thông tin nhạy cảm, nhưng cũng có thể là do vô ý, chẳng hạn như lỗi người dùng khiến hệ thống tạm thời không hoạt động. Ngoài ra, các rủi ro cũng có thể đến từ các nguồn bên ngoài của tổ chức, chẳng hạn như tội phạm mạng và các đối tác tham gia trong chuỗi cung ứng, hoặc các rủi ro đến từ các nguồn bên trong tổ chức như nhân viên và nhà quản lý. Vì thế theo cách tiếp cận này, rủi ro an ninh mạng bao gồm:

- Rủi ro do cố ý từ bên trong: tức là các hành vi cố ý phá hoại, trộm cắp hoặc hành vi xấu khác do nhân viên và những người khác trong tổ chức đã thực hiện. Ví dụ, một nhân viên bất mãn xóa thông tin quan trọng trước khi họ rời tổ chức.
- Rủi ro do vô ý từ bên trong: tức là hành vi vô ý dẫn đến thiệt hại hoặc mất mát do nhân viên và người khác trong tổ chức. Ví dụ: vào năm 2013, NASDAQ đã gặp sự cố công nghệ do nội bộ gây ra khiến hệ thống sao chép bị lỗi (McCrank J., 2013).
- Rủi ro do cố ý từ bên ngoài: đây là loại rủi ro an ninh mạng phổ biến nhất. Các cuộc tấn công mạng đều được thực hiện do các cá nhân hoặc tổ chức bên ngoài, bao gồm cả các tổ chức tội phạm hoặc những người theo chủ nghĩa Hacktivism (chủ nghĩa tin tặc). Ví dụ, các cuộc tấn công mạng theo hình thức từ chối dịch vụ phân tán (DoS) làm giảm hiệu suất của các thiết bị công nghệ và của cả hệ thống CNTT.
- Rủi ro do vô ý từ bên ngoài: Tương tự như hành vi vô ý từ bên trong, những hành vi vô ý từ bên ngoài tổ chức cũng có thể gây thiệt hại cho tổ chức. Ví dụ: hệ thống kỹ thuật của công ty ngừng hoạt động do bên đối tác gặp sự cố kỹ thuật, do tin tặc tấn công hoặc do thiên tai gây ra.

Tuy nhiên có thể thấy, dù được phân loại theo cách tiếp cận nào đi chăng nữa thì các loại rủi ro an ninh mạng đều gây ra thiệt hại cho một tổ chức, bao gồm: *thiệt hại danh tính, rò rỉ thông tin và làm gián đoạn quá trình kinh doanh*. Quan điểm này cũng được Hiệp hội Bảo hiểm Quốc gia Mỹ sử dụng trong việc xác định các thiệt hại do rủi ro an ninh mạng gây ra (Biener, Eling và Wirfs, 2015).

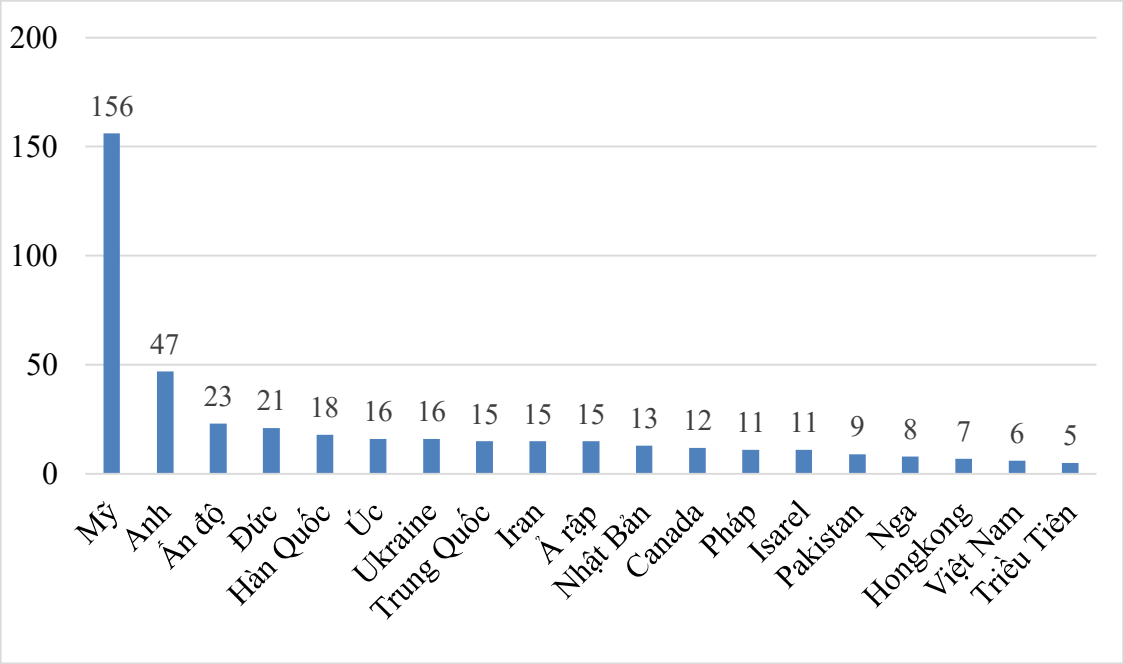
2.3. Tình hình về rủi ro an ninh mạng trên thế giới

Trong những năm gần đây, rủi ro an ninh mạng ngày càng thu hút sự quan tâm của mọi tổ chức trên thế giới. Theo khảo sát của tổ chức DTCC (2020), rủi ro an ninh mạng trở thành mối quan ngại hàng đầu, ảnh hưởng đến sự ổn định của hệ thống tài chính toàn cầu, chỉ đứng sau đại dịch do Covid-19 gây ra. Theo Báo cáo về Rủi ro Toàn cầu 2020 của đàn kinh tế thế giới (WEF, 2020a), rủi ro do các cuộc tấn công mạng vào cơ sở hạ tầng CNTT và gian lận hoặc đánh cắp dữ liệu được xếp vào một trong 10 loại rủi ro hàng đầu có khả năng xảy ra nhất. Trong khi đó, dự báo rủi ro liên quan đến Covid-19 của WEF (2020b) cho rằng tấn công mạng là mối quan tâm lớn đứng thứ ba của công dân toàn cầu khi xu hướng chuyển dịch sang các mô hình làm việc từ xa do đại dịch gây ra.

Dữ liệu thống kê cho thấy những mối quan tâm này là hoàn toàn có cơ sở. Theo báo cáo về tội phạm mạng gần đây của FBI, kể từ khi đại dịch Covid-19 bắt đầu, một số loại tấn công mạng đã tăng hơn 300% và chi phí liên quan của một số tội phạm tăng hơn 2,400% (WEF, 2020). Điển hình lừa đảo qua mạng (Phishing) tăng cao từ 26,379 vào năm 2018 lên đến 241,342 vụ trong năm 2020. Xu hướng này cũng được Google nhấn mạnh, cho thấy mỗi ngày công ty đã chặn hơn 18 triệu nỗ lực lừa đảo bằng cách ghi tên Corona lên các tệp hoặc link chứa mã độc (FBI, 2020). Ngoài ra, theo tổ chức Cybersecurity Ventures, thiệt hại do tội phạm mạng ước tính lên tới 6 nghìn tỷ đô la Mỹ vào năm 2021 và 10.5 nghìn tỷ USD vào năm 2025 so với chỉ 3 nghìn tỷ vào năm 2015. Con số này tương đương với GDP của nền kinh tế lớn thứ ba thế giới chỉ sau Mỹ và Trung Quốc (Steve Morgan, 2021). Bên cạnh chi phí tài chính, các cuộc tấn công mạng làm suy giảm niềm tin của người sử dụng. Các cuộc khảo sát chỉ ra rằng trong số người có truy cập Internet trên toàn cầu, chưa đến 50% tin tưởng rằng công nghệ sẽ cải thiện cuộc sống của họ. Điều này cho thấy việc thiếu tin tưởng ngày càng gia tăng về tính bảo mật và đảm bảo quyền riêng tư của người dùng. Ví dụ, khảo sát của Accenture (2020) cũng cho thấy 68% lãnh đạo doanh nghiệp cảm thấy rủi ro an ninh mạng đang gia tăng khi có ngày càng nhiều doanh nghiệp và người dân dựa vào Internet để thực hiện các hoạt động hàng ngày của mình.

Tuy nhiên, trước khi đại dịch xảy ra thì các vụ tấn công mạng cũng đã là vấn đề gây lo lắng cho chính phủ các nước. Theo luật pháp Mỹ, tội phạm mạng có thể nhận án tù lên đến 20 năm nếu tấn công vào cơ quan chính phủ và làm ảnh hưởng đến an ninh quốc gia. Mặc dù đã gia tăng các hình phạt

và mức phạt tù nhưng điều đó có vẻ như không ảnh hưởng đến sự gia tăng số lượng tội phạm mạng ở quốc gia này. Theo thống kê về những vụ tấn công mạng trong giai đoạn 5/2006-06/2020 của Trung tâm nghiên cứu và chiến lược quốc tế (Centre for Strategic and International Studies-CSIS), Mỹ là quốc gia đứng đầu trong danh sách bị tấn công mạng. Cụ thể, trong tổng số 424 vụ tấn công mạng (có mức thiệt hại hơn 1 triệu USD) ở 20 quốc gia trong vòng gần 15 năm qua, gần 50% (156 vụ) là xảy ra ở Mỹ (xem chi tiết hình) và riêng năm 2018 là tệ nhất khi có đến 30 vụ tấn công mạng ở Mỹ (Carmen Ang, 2021).



Hình 2: Thống kê các vụ tấn công mạng ở 20 quốc gia trên thế giới (chỉ tính các vụ gây thiệt hại hơn 1 triệu USD)

Nguồn: Carmen Ang (2021)

Trong số các vụ tấn công mạng trong thời gian qua, có 4 loại phổ biến nhất, bao gồm (i) tấn công bằng ngôn ngữ lập trình cấu trúc SQL, (ii) tấn công trung gian (MitM), lừa đảo thông qua email (phishing) và tấn công từ chối dịch vụ (DoS). Dữ liệu thống kê từ các tổ chức quốc tế cũng cho thấy các hình thức tấn công mạng này cũng không ngừng gia tăng trong khoảng thời gian gần đây. Ví dụ, CISO dự đoán các vụ tấn công từ chối dịch vụ (DOS) sẽ tăng gấp đôi so với năm 2018, thiệt hại lên đến 15.4 triệu USD vào năm 2023 (Steve Morgan, 2019).

Dưới đây là thống kê một số vụ tấn công mạng điển hình (Johnathan Greg, 2019; Cyberreef, 2020):

- Vào giữa tháng 5 năm 2017, một loại mã độc với tên gọi WannaCry đã tấn công vào hệ thống mạng ở 150 quốc gia khiến cho nhiều tập tin của người dùng bị khóa. Nếu muốn có quyền mở khóa, nạn nhân phải trả cho các hacker giá trị bitcoin 300 USD. Sau 72 giờ kể từ ngày đầu tiên của cuộc tấn công này, khoản tiền này sẽ được tăng lên gấp đôi ở mức 600 USD giá trị bitcoin, và sau bảy ngày thì các tập tin sẽ bị khóa vĩnh viễn.
- Vào tháng 6 năm 2017, hàng loạt doanh nghiệp tại Ukraine báo cáo đã bị một loại mã độc có tên NotPetya tấn công. Mã độc này sau đó lan sang các doanh nghiệp lớn trên toàn cầu bao gồm FedEx, tập đoàn dầu khí khổng lồ của Rosneft ở Nga và hãng vận tải Maersk của Đan Mạch. Trong tháng 9 năm 2017, FedEx ước tính mức thiệt hại lên tới 300 triệu USD do cuộc tấn công mạng này gây ra.
- Vào tháng 6 năm 2020, có một cuộc tấn công mạng quy mô lớn chống lại 9 nhà hoạt động nhân quyền ở Ấn Độ. Để làm được điều đó, tội phạm mạng đã cài đặt phần mềm vào các máy tính cá nhân của những nhà hoạt động nhân quyền này để giúp chúng đánh cắp các thông tin đăng nhập và ghi âm lại tất cả các lần gõ phím của họ.
- Vào tháng 12 năm 2020, một trong những hãng truyền thông lớn nhất ở Đức, Funke Media Group, trở thành nạn nhân của một cuộc tấn công bằng mã độc. Khoảng 6,000 máy tính đã bị nhiễm độc, khiến công việc tại các văn phòng biên tập cũng như một số nhà in lớn của công ty phải tạm dừng hoạt động.

2.4. Tình hình rủi ro an ninh mạng trong lĩnh vực tài chính ngân hàng

So với các ngành khác, lĩnh vực tài chính thường xuyên bị tấn công mạng đặc biệt kể từ khi đại dịch diễn ra. Điều này có thể xuất phát từ tính đặc thù của ngành. Bởi vì hoạt động của các tổ chức tài chính thường phụ thuộc rất lớn vào cơ sở hạ tầng CNTT và đặc biệt là sự kết nối thông tin trong tổ chức.

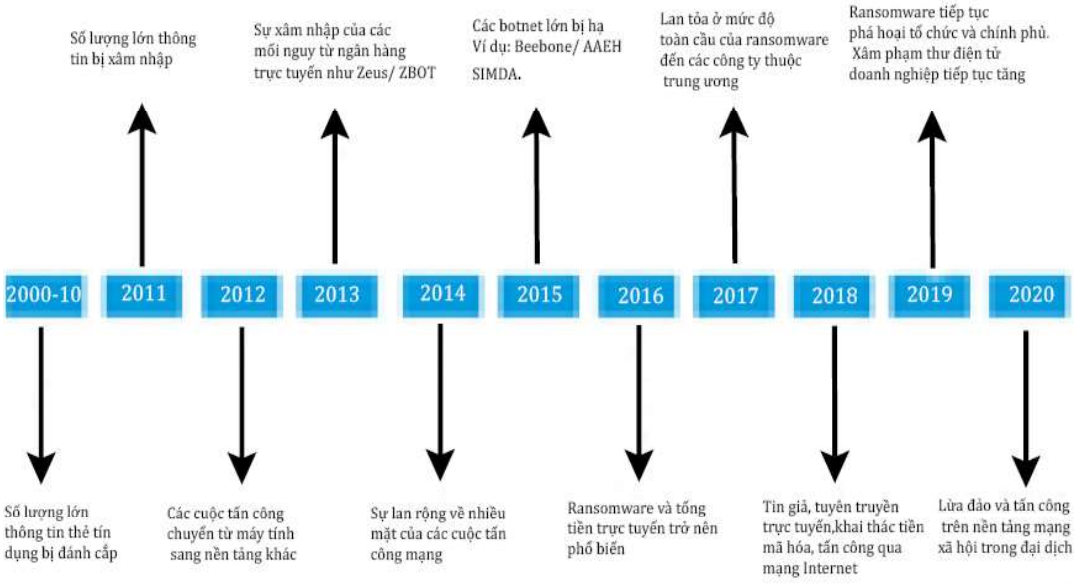
Trong báo cáo về tổn thất vi phạm dữ liệu trên phạm vi toàn cầu do IBM (2020) thực hiện, chỉ tính riêng ngành dịch vụ tài chính đã thiệt hại 5.85 triệu USD cho các tổn thất vi phạm dữ liệu. Trong số 17 ngành công nghiệp được IBM thực hiện khảo sát, ngành tài chính đứng thứ ba về chi phí tổn thất trung bình. Số liệu từ khảo sát toàn cầu về An ninh mạng của Keepersecurity (2020) cũng khẳng định điều đó. Cụ thể, 70% tổ chức tài chính đã từng là nạn nhân của các cuộc tấn công mạng. Cuộc khảo sát cũng cho biết các vi phạm dữ liệu trong các dịch vụ tài chính đã khiến trung bình 7,095 hồ sơ khách hàng và nhân viên bị mất hoặc bị đánh cắp, đồng thời gây thiệt hại trung bình 1.06 triệu USD do gián đoạn hoạt động kinh doanh. Ngoài ra, báo cáo cập nhật về an ninh mạng của Insights (2021) cũng cho thấy hơn 25% các cuộc tấn công bằng phần mềm độc hại là nhắm vào các ngân hàng và tổ chức dịch vụ tài chính; số lượng này nhiều hơn bất kỳ ngành nào khác. Cũng theo thông tin công bố trong báo cáo, số lượng thẻ tín dụng bị tội phạm mạng tấn công đã tăng rất cao so với các năm trước đó (212%), tương tự là số lượng vụ tấn công mạng liên quan đến rò rỉ thông tin xác thực (129%) và cài đặt các ứng dụng độc hại (102%).

Dưới đây là một vài ví dụ tấn công mạng có liên quan đến ngân hàng và hệ thống tài chính (Antoine Bouveret, 2018; Iñaki Aldasoro và cộng sự, 2021).

- Trong năm 2016, ngân hàng Tesco có trụ sở tại Anh thông báo rằng 20,000 khách hàng của ngân hàng đã bị đánh cắp tới 2,000 bảng Anh từ tài khoản của mình trong một cuộc tấn công mạng.
- Tương tự, trong năm 2016, ngân hàng trung ương Bangladesh đã bị tấn công bởi tin tặc mà FBI quy trách nhiệm cho Triều Tiên. Vào tháng 2 năm 2019, Bộ Tư pháp đã buộc tội ba người Triều Tiên âm mưu tống tiền và đánh cắp hơn 1.3 tỷ đô la tiền mặt và tiền điện tử từ các ngân hàng và các doanh nghiệp khác.
- Sau đó, vào tháng 12 năm 2019, các công tố viên của Hoa Kỳ đã buộc tội hai công dân Nga với tội danh rất nghiêm trọng (được xem là một trong những tội phạm mạng lớn nhất trong lịch sử). Bởi vì, Igor Turashev và Maksim Yakubets đã tiến hành một cuộc tấn công DDoS vào một ngân hàng và một số tổ chức khác có trụ sở tại Pennsylvania. Hai tin tặc này được cho rằng đã chiếm đoạt hơn 3 triệu USD và phải chịu trách nhiệm thêm cho hàng chục triệu USD thiệt hại.

- Gần đây hơn, vào tháng 8 năm 2020, một số cơ quan chính phủ, bao gồm FBI, Bộ Tài chính, Bộ Chỉ huy Mạng Hoa Kỳ báo cáo rằng một nhóm tin tặc Bắc Triều Tiên đã đánh cắp hàng chục triệu USD từ các ngân hàng và tổ chức tài chính chỉ riêng trong năm 2020. Bên cạnh những thiệt hại về tài chính, những kẻ tấn công đã hack vào máy ATM, làm gián đoạn dịch vụ rút tiền trong nhiều tuần hoặc nhiều tháng của các tổ chức này (FinTech News, 2020).

Hình dưới đây mô tả sự thay đổi trong tính chất các vụ tấn công mạng ở lĩnh vực tài chính ngân hàng trong 10 năm. Biểu đồ cũng cho thấy mức độ phức tạp của các cuộc tấn công mạng trong lĩnh vực này.



Hình 3: Sự phát triển của các hình thức tấn công mạng từ 2010-2020

Nguồn: Frank Adelmann và cộng sự (2020)

3. HOẠT ĐỘNG NGÂN HÀNG SỐ

3.1. Khái quát về ngân hàng số

Ngân hàng số là thuật ngữ dùng để chỉ mô hình ngân hàng dựa trên nền tảng cộng nghệ mà cho phép số hóa tất cả sản phẩm và dịch vụ ngân hàng truyền thống (Skinner, 2014). Nói cách khác, ngân hàng số là một mô hình kinh doanh dựa trên nền tảng công nghệ để trao đổi thông tin và thực hiện giao dịch giữa các ngân hàng và khách hàng. Tất cả các dịch vụ ngân hàng như chuyển khoản, gửi tiền tiết kiệm, quản lý tài khoản, cho vay và tư vấn đầu tư đều được số hóa và tích hợp vào ngân hàng số. Tất cả các dịch vụ này có thể được truy cập thông qua các trang web hoặc thiết bị di động.

Khi đó, khách hàng không cần phải đến chi nhánh ngân hàng để thực hiện giao dịch và ngược lại, ngân hàng cũng không phải gặp khách hàng để hoàn thành giao dịch. Khi đó, thời gian thực hiện và tương tác giữa khách hàng và ngân hàng sẽ được rút ngắn và qua đó tối ưu hoá được giao dịch.

Có một số quan điểm cho rằng, ngân hàng số (digital banking) có nhiều điểm tương đồng với ngân hàng điện tử (e-banking). Bởi vì, cả hai loại hình đều ứng dụng công nghệ hiện đại vào hoạt động kinh doanh ngân hàng. Cả hai cũng đều hướng đến tính hiệu quả và thuận tiện khi cung cấp sản phẩm dịch vụ ngân hàng trực tuyến cho khách hàng. Tuy nhiên, ngân hàng số là mô hình kinh doanh bao quát hơn nhiều so với ngân hàng điện tử (e-banking). Ví dụ, ngân hàng điện tử chỉ tập trung vào số hóa một số tính năng trên nền tảng ngân hàng truyền thống với các dịch vụ như: Internet Banking, SMS Banking. Trong khi đó, ngân hàng số hướng đến số hoá tất cả các hoạt động của ngân hàng (SCN Education B.V., 2001). Cho nên, có thể thấy ngân hàng số là một mô hình ngân hàng hiện đại hơn so với ngân hàng điện tử.

Về cơ bản, mô hình kinh doanh của ngân hàng số sẽ bao gồm tất cả các khía cạnh, lĩnh vực hoạt động của một ngân hàng thông thường như tổ chức, quản lý nguồn nhân lực, cung cấp và xử lý các hoạt động và dịch vụ tài chính (Kelman, 2016). Ngân hàng số cũng sẽ có nhiều tính năng ưu việt như dịch vụ 24/7 với mọi giao dịch thông qua Internet và các ứng dụng công nghệ và đặc biệt tất cả các thủ tục hành chính đều được số hóa và đơn giản hóa. Ở mức độ nhất định, ngân hàng số cũng có thể được coi là ngân hàng không chi nhánh hoặc ngân hàng tự động (Scardovi, 2017).

3.2. Xu hướng phát triển ngân hàng số tại Việt Nam

Hiện nay, hầu hết các ngân hàng Việt Nam đang thực hiện chuyển đổi số. Theo kết quả khảo sát của Ngân hàng Nhà nước (NHNN) vào tháng 9/2020, 95% ngân hàng đã và đang xây dựng chiến lược chuyển đổi số. Trong đó, gần 42% ngân hàng đang xây dựng chiến lược chuyển đổi số và khoảng 40% ngân hàng đã phê duyệt chiến lược chuyển đổi số hoặc tích hợp trong chiến lược phát triển kinh doanh/CNTT (Phạm Tiến Dũng, 2021). Trong chiến lược chuyển đổi số, đa số các ngân hàng đều lựa chọn chuyển đổi số cả kênh giao tiếp khách hàng (front-end) và quy trình nghiệp vụ nội bộ (back-end) hoặc số hóa toàn bộ hoạt động ngân hàng; một số ít ngân hàng dự kiến chỉ số hóa kênh giao tiếp khách hàng (front-end only).

Về công nghệ, hầu hết các ngân hàng đều ứng dụng các giải pháp kỹ thuật, công nghệ mới như điện toán đám mây, phân tích dữ liệu lớn (Big data), tự động hóa quy trình bằng robot, trí tuệ nhân tạo (AI), công nghệ Blockchain, nhận biết và định danh khách hàng bằng eKYC,... trong các hoạt động nghiệp vụ và cung ứng sản phẩm, dịch vụ để nâng cao hiệu quả hoạt động và tăng trải nghiệm khách hàng. Trong đó, công nghệ dữ liệu, trí tuệ nhân tạo được các ngân hàng áp dụng nhiều nhất trong phân tích hành vi và nhu cầu khách hàng; qua đó giúp ngân hàng tối ưu hóa, cá nhân hóa việc cung ứng sản phẩm, dịch vụ của mình. Hệ thống ngân hàng lõi và hạ tầng công nghệ cũng được các ngân hàng chú trọng đầu tư và nâng cấp nhằm đảm bảo hoạt động ổn định, an toàn và đáp ứng nhu cầu phát triển. Vấn đề an ninh mạng và bảo mật thông tin cũng được coi trọng và tăng cường để nâng cao chất lượng dịch vụ, tạo sự yên tâm cho khách hàng khi sử dụng các dịch vụ ngân hàng số hoặc ngân hàng điện tử.

Nhiều ngân hàng cũng đã xây dựng kho dữ liệu, hạ tầng số tập trung, chuẩn hóa, cho phép chia sẻ, tích hợp, tạo hệ sinh thái số trải rộng ở nhiều ngành, lĩnh vực như: hệ sinh thái ngân hàng số kết nối với dịch vụ công, tài chính, viễn thông, điện lực, giao thông, y tế... nhờ đó, trên ứng dụng di động của ngân hàng, khách hàng có thể sử dụng được nhiều tiện ích hơn so với giao dịch trực tiếp tại ngân hàng. Riêng đối với dịch vụ ngân hàng trên điện thoại di động (Mobile Banking) đã đạt được kết quả ấn tượng với mức tăng trưởng thanh toán di động năm 2020 tăng 123.9% về giá trị và 125.4% về số lượng so với 2019, thanh toán QR code tăng 82.4% về số lượng giao dịch. Số lượng, giá trị giao dịch ngân hàng qua kênh số của nhiều ngân hàng Việt Nam có sự tăng trưởng vượt bậc; một số ngân hàng như TPBank, MB đã ghi nhận tỷ lệ hơn 80% giao dịch được thực hiện trên nền tảng số (Phạm Tiến Dũng, 2021).

Tóm lại, về xu hướng phát triển ngân hàng số, hiện có 2 cách tiếp cận khác nhau ở Việt Nam. Cách tiếp cận đầu tiên chủ yếu thực hiện thông qua quá trình số hóa một ngân hàng hiện có, có thể số hoá quy trình nội bộ, sản phẩm kinh doanh hoặc các kênh phân phối. Ví dụ số hoá kênh phân phối thể hiện ở sự tích hợp các ứng dụng công nghệ trong cung cấp dịch vụ ngân hàng trên thiết di động, chính sách định danh khách hàng (eKYC), thanh toán bằng mã QR, trợ lý ảo/chatbots và trung tâm liên lạc 24/7. Trong khi đó, số hoá quy trình nội bộ thường được thực hiện ở hệ thống giao dịch trực tuyến, quy trình xử lý tự động hóa bằng robot và ứng dụng trí tuệ nhân tạo AI trong quản lý rủi ro ngân hàng. Mặc dù đã có một số kết quả nhất định

nhưng có thể thấy hiện nay quá trình số hóa ngân hàng và đặc biệt việc sử dụng công nghệ và các công cụ phân tích và quản lý dữ liệu như tự động hoá trong thu thập dữ liệu, điện toán đám mây, phân tích dữ liệu lớn, API mở và ứng dụng công nghệ AI và blockchain vẫn còn ở giai đoạn sơ khai.

Ví dụ, Vietcombank, Techcombank và MBBank là một số ngân hàng đang thực hiện theo cách tiếp cận đầu tiên đối với ngân hàng số. Trong đó, các ngân hàng này phát triển hoạt động ngân hàng số trên một nền tảng ứng dụng đa kênh. Ngoài ra, các công cụ phân tích dữ liệu tiên tiến cũng được sử dụng để phân tích hành vi của khách hàng; qua đó cho phép các sản phẩm và dịch vụ của họ có thể tiếp cận được khách hàng một cách nhanh chóng và vì thế có được lợi thế cạnh tranh trên thị trường.

Cách tiếp cận thứ hai là sự kết hợp của cách tiếp cận đầu tiên cùng với sự phát triển của các ngân hàng kỹ thuật số độc lập. Xu hướng này xuất hiện ở một số ngân hàng như TPBank với ứng dụng LiveBank; VPBank với ngân hàng số Timo, cũng như Yolo mới ra mắt gần đây. Mới đây nhất, Ngân hàng TMCP Nam Á (Nam A Bank) chính thức ra mắt không gian giao dịch số tích hợp hệ sinh thái thiết bị hiện đại, ứng dụng trí tuệ nhân tạo (AI) với sự xuất hiện của Robot OPBA và chi nhánh số VTM OPBA.

Tuy nhiên, phát triển ngân hàng số ở Việt Nam vẫn còn nhiều khó khăn. Điển hình là hành lang pháp lý về ngân hàng số hiện nay chưa đầy đủ và thường đi sau sự phát triển công nghệ. Ví dụ hệ thống thông tin điện tử cơ bản của công dân chưa hoàn thiện; chưa có văn bản pháp lý hoàn thiện cho các vấn đề như định danh điện tử, văn bản số (văn bản điện tử), hay chữ ký điện tử… Việt Nam chưa có chuẩn QR chung cho việc liên thông thanh toán.

4. ẢNH HƯỞNG CỦA RỦI RO AN NINH MẠNG ĐẾN HOẠT ĐỘNG NGÂN HÀNG SỐ Ở VIỆT NAM

Tội phạm mạng là các hoạt động bất hợp pháp thông qua các máy tính trung gian được thực hiện bởi một số bên trên không gian mạng (Douglas and Loader, 2000). Trong lĩnh vực ngân hàng, các loại tội phạm mạng bao gồm xâm nhập bất hợp pháp (cyber-trespass/hacking and cracking) và lừa dối mạng (bẫy mạng) (cyber-deceptions/thefts) (Wall, 2001). Các hành vi lừa dối (gian lận) phổ biến như là gian lận thẻ tín dụng, gian lận tiền điện tử, xóa hoặc chuyển tiền bất hợp pháp đến các tài khoản khác nhau và vi phạm bản quyền mạng (Wall, 2001).

Theo báo cáo của Goud (2019), Việt Nam nằm trong danh sách các nước bị gián điệp mạng tấn công nhiều nhất với vị trí thứ 6 trên toàn cầu

(bảng 1). Đồng thời, Việt Nam cũng đứng thứ 8 trong danh sách các quốc gia bị tấn công từ chối dịch vụ (DDoS) nhiều nhất (bảng 2).

Bảng 1: Danh sách các quốc gia bị gián điệp mạng tấn công nhiều nhất

Thứ hạng	Quốc gia	Tỷ trọng (%)
1	Mỹ	54
2	Hàn Quốc	6
3	Nhật Bản	4
4	Nga	3
5	Columbia và Ukraine	2
6	Việt Nam, Belarus, Kazakhstan và Philippines	1

Nguồn: Goud (2019)

Bảng 2: Danh sách các quốc gia bị tấn công từ chối dịch vụ (DDoS) nhiều nhất

Thứ hạng	Quốc gia	Tỷ trọng
1	Trung Quốc	29.56
2	Mỹ	21.59
3	Anh	16.17
4	Pháp	8.72
5	Hàn Quốc	4.06
6	Singapore	3.93
7	Nhật Bản	3.81
8	Việt Nam	3.76
9	Đức	3.49

Nguồn: Goud (2019)

Theo báo cáo của Apcert, trong giai đoạn từ 2013-2020, Việt Nam có số vụ tấn công mạng tăng nhanh từ hơn 6,000 vụ năm 2013 lên đến hơn 15,000 vụ năm 2015. Năm 2016, số vụ tấn công đã gia tăng đột biến lên đến 134 ngàn, tăng gấp 9 lần so với năm trước đó. Sau đó, số vụ tấn công đã giảm xuống đáng kể chỉ còn hơn 5,000 vụ trong năm 2019. Tuy nhiên, sang năm 2020, số vụ tấn công mạng lại có xu hướng tăng lên đáng kể với hơn 11,000 vụ (bảng).

Bảng 3: Số vụ tấn công an ninh mạng ở Việt Nam giai đoạn 2013-2020

Sự cố an ninh mạng	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Lừa đảo (phishing)	2,469	1,458	5,104	10,057	2,605	2,611	3,167	2,025
Tấn công thay đổi giao diện (deface)	1,603	8,291	6,188	77,654	4,377	5,297	1,432	6,801
Phần mềm độc hại (malware)	2,142	10,037	3,885	46,664	6,400	1,758	577	2,556
Tổng	6,214	19,786	15,177	134,375	13,382	9,666	5,176	11,382

Nguồn: Apcert (2020)

Theo đánh giá của tập đoàn công nghệ Bkav, virus máy tính đã gây ra thiệt hại kỷ lục cho người dùng Việt Nam trong năm 2020, với con số trên 1 tỷ USD (23.9 nghìn tỷ đồng) (Lâm Thảo, 2020). Theo khảo sát của Hiệp hội An toàn thông tin Việt Nam, hơn 50% các cuộc tấn công mạng là nhằm vào các tổ chức tài chính và ngân hàng (Hà An, 2020). Theo báo cáo của Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Bộ Công an, trong năm 2020 các vụ tấn công an ninh mạng đã gây ra thiệt hại khoảng 100 tỷ đồng, trong đó có ngân hàng bị thiệt hại tới 44 tỷ đồng (Huyền Anh, 2020). Các vụ tấn công mạng vào các ngân hàng ở Việt Nam rất đa dạng và tinh vi. Chẳng hạn như, tội phạm mạng đã sử dụng các tin nhắn mạo danh các ngân hàng (ACB, Vietcombank, Techcombank, SCB) để lừa khách hàng cung cấp các thông tin tài khoản ngân hàng như số tài khoản ngân hàng, tên tài khoản, mật khẩu và mã xác thực OTP. Gần đây,

ngân hàng Nông nghiệp và phát triển nông thôn Việt Nam cũng bị tội phạm mạng dùng các website, các trang điện tử giả mạo ngân hàng nhằm đánh cắp thông tin và lấy cắp tiền của khách hàng. Tội phạm mạng tấn công vào ngân hàng bằng các phương thức phổ biến sau: (i) Trộm cắp dữ liệu của ngân hàng, thông tin tài khoản khách hàng và thông tin thẻ tín dụng; (ii) Lừa đảo thông qua email để lấy cắp thông tin tài khoản; (iii) Xâm nhập vào hệ thống thông qua kẽ hở trong quy trình, lỗ hổng bảo mật để chiếm quyền quản trị hệ thống; (iv) Tấn công cơ sở dữ liệu và chiếm quyền điều khiển hệ thống nhằm lấy cắp tiền của ngân hàng (Ngọc Khang, 2021).

Với xu hướng phát triển ngân hàng số ở Việt Nam hiện nay, ngành ngân hàng phải đối mặt với những thách thức về an ninh mạng như: hệ thống dữ liệu ngân hàng bị tấn công thông qua các đối tác của ngân hàng; các website bị thay đổi giao diện và bị xâm nhập để lấy cắp dữ liệu và chiếm đoạt thông tin; hệ thống bị xâm nhập bất hợp pháp để thực hiện các lệnh chuyển tiền gây thiệt hại về tài sản của ngân hàng và khách hàng; các vụ tấn công nhằm vào các khách hàng của ngân hàng như lừa mất tiền qua tài khoản, mạo danh nhân viên ngân hàng để lừa tiền khách hàng hoặc gửi link giả mạo ngân hàng, các website mạo danh ngân hàng được lập ra để lừa đảo khách hàng... Như vậy, ngân hàng số ở Việt Nam đứng trước rủi ro an ninh mạng rất cao vì cả ba chủ thể tham gia vào hoạt động ngân hàng số bao gồm ngân hàng, các đối tác của ngân hàng và các khách hàng đều có thể là mục tiêu tấn công của tội phạm mạng. Đây cũng chính là các cửa ngõ mà tội phạm mạng có thể dùng để tấn công vào ngân hàng.

5. THÁCH THỨC TRONG QUẢN LÝ RỦI RO AN NINH MẠNG

Thứ nhất, việc bảo đảm an toàn an ninh mạng phụ thuộc rất lớn vào công nghệ và đòi hỏi các ngân hàng phải đầu tư đáng kể cho hệ thống hạ tầng CNTT. Mặc dù, các ngân hàng, đặc biệt là ngân hàng số, đã chú trọng đầu tư nhưng một số ngân hàng chưa đầu tư đồng bộ để nâng cấp hệ thống, hoặc chưa trang bị các phiên bản hiện đại nhất có khả năng phát hiện các bất thường. Do đó, số vụ tấn công vào ngân hàng nói chung và ngân hàng số nói riêng vẫn tăng cao.

Thứ hai, mặc dù các NHTM ở Việt Nam đã chú trọng đến an ninh mạng, một số ngân hàng vẫn chưa kiện toàn bộ phận nhân sự cấp cao chuyên phụ trách xử lý vấn đề rủi ro an ninh mạng như giám đốc an ninh thông tin (CISO). Thực tế là quản trị rủi ro an ninh mạng là công việc rất phức tạp, không chỉ đòi hỏi giám đốc phải có kinh nghiệm trong quản lý

còn đòi hỏi họ phải có kinh nghiệm về an ninh mạng, về CNTT để có thể ra các quyết định đúng đắn trong việc xác định các tài sản ưu tiên cần bảo vệ, nguy cơ, cũng như các lỗ hổng an ninh mạng của ngân hàng.

Thứ ba, nhiều ngân hàng chưa xây dựng quy trình quản trị rủi ro an ninh mạng mang tính đồng bộ và hiệu quả. Thiếu hẳn các kịch bản ứng phó với các sự cố, rủi ro mất an toàn thông tin và quy trình xử lý nhằm làm giảm các tác động tiêu cực, hậu quả của các cuộc tiến công mạng vẫn chưa được chú trọng. Bên cạnh đó, ngân hàng thiếu các quy trình xử lý sự cố khi khách hàng gặp rủi ro an ninh mạng. Chính vì vậy, nhân viên ngân hàng còn lúng túng trong việc xử lý sự cố, điều này dễ dẫn tới sụt giảm niềm tin của khách hàng.

Thứ tư, cách thức sử dụng công nghệ của các bên liên quan (ví dụ như nhà cung cấp và khách hàng của ngân hàng) cũng ảnh hưởng quan trọng đến vấn đề đảm bảo an toàn an ninh mạng. Hiện nay, các đối tác của ngân hàng chưa đặc biệt chú trọng đến vấn đề an ninh mạng, thậm chí có những đối tác chưa đủ năng lực và hạ tầng về an toàn thông tin. Chẳng hạn như, thời gian gần đây, các khách hàng của ngân hàng bị tấn công chỉ từ email quảng cáo hoặc tin nhắn mà ngân hàng thuê đối tác thực hiện.

Thứ năm, nhiều khách hàng chưa có ý thức bảo vệ thông tin cá nhân như số chứng minh nhân dân, số tài khoản ngân hàng, số điện thoại, hay ngày tháng năm sinh... các thông tin của khách hàng có thể được lưu lại trên mạng xã hội thông qua các giao dịch mua, bán hàng online và dễ dàng được tội phạm mạng thu thập. Theo thống kê của Bkav, có khoảng 55% người dùng vẫn sử dụng chung một mật khẩu cho các tài khoản tại nhiều dịch vụ trực tuyến khác nhau. Đây chính là kẽ hở để tội phạm dễ dàng xâm nhập, tấn công và đánh cắp tài khoản (Nguyễn Vũ, 2019). Bên cạnh đó, tội phạm mạng còn đánh cắp thông tin của khách hàng thông qua các hình thức phát tán virus, phát tán các mã độc được cài đặt trong các email, phần mềm miễn phí hay mạng xã hội mà khách hàng sử dụng. Với thông tin cá nhân của khách hàng, tội phạm mạng dễ dàng thực hiện lừa đảo trực tuyến, mua bán, sử dụng trái phép thông tin khách hàng.

Thứ sáu, mặc dù đã có nhiều nỗ lực trong kiện toàn hành lang pháp lý cho hoạt động ngân hàng số nhưng hiện vẫn còn nhiều thiếu sót. Ví dụ, chưa có các quy định pháp lý cho các vấn đề về định danh và xác thực điện tử cũng như các vấn đề liên quan đến bảo vệ quyền riêng tư dữ liệu người dùng trong môi trường mạng. Hiện cũng chưa có cơ chế cho phép các ngân

hàng được kết nối và khai thác, chia sẻ thông tin trực tuyến để phục vụ cho việc xác minh thông tin khách hàng bằng phương thức điện tử.

6. ĐỀ XUẤT MỘT SỐ KIẾN NGHỊ VÀ GIẢI PHÁP NHẰM GIẢM THIỂU RỦI RO AN NINH MẠNG TRONG HOẠT ĐỘNG NGÂN HÀNG SỐ TẠI VIỆT NAM

6.1. Kiến nghị với Chính phủ

Một là, tiếp tục hoàn thiện cơ sở pháp lý về phòng, chống tội phạm sử dụng công nghệ cao.

Quán triệt, thực hiện Luật an toàn thông tin mạng 2015, Luật An ninh mạng 2018, Nghị định 85/2016 về an toàn hệ thống thông tin theo cấp độ, Nghị định số 04/2019/NĐ-CP quy định về trình tự, thủ tục áp dụng một số biện pháp bảo đảm an ninh mạng. Tiếp tục nghiên cứu hoàn thiện hệ thống các văn bản pháp luật liên quan đến tội phạm mạng để có thể theo kịp với sự biến đổi nhanh chóng của công nghệ cũng như tình hình tội phạm mạng diễn biến ngày càng tinh vi, phức tạp. Nghiên cứu, áp dụng các tiêu chuẩn, thông lệ quốc tế về an ninh, an toàn hệ thống thông tin, khung đánh giá rủi ro CNTT vào các văn bản quy phạm pháp luật điều chỉnh hoạt động ứng dụng CNTT. Đặc biệt chú trọng các quy định chế tài cụ thể, rõ ràng hơn trong việc xử lý đối với các hành vi vi phạm trong lĩnh vực ứng dụng công nghệ cao tại Việt Nam.

Hai là, xây dựng và cụ thể hoá các hành động trong chiến lược an ninh mạng ở tầm quốc gia.

Điều này sẽ giúp Chính phủ chủ động trong bảo vệ an ninh quốc gia, hỗ trợ các hoạt động kinh tế, xã hội và đặc biệt là thúc đẩy niềm tin người dùng và sự tự tin trong kinh doanh trên không gian mạng. Ví dụ, ở Đan Mạch, trong chiến lược an ninh mạng quốc gia, Chính phủ thiết lập một cổng thông tin (https://sikkerdigital.dk/) dành riêng cho việc chia sẻ thông tin và hợp tác trong phòng ngừa rủi ro an ninh mạng. Trên cổng thông tin chuyên biệt này, công dân, doanh nghiệp và các cơ quan ban ngành có thể truy xuất các thông tin và các công cụ đề xuất trong xử lý liên quan đến vấn đề an toàn an ninh mạng, cũng như đảm bảo việc tuân thủ pháp luật về an ninh mạng. Ngoài ra, cổng thông tin cũng luôn được cập nhật thường xuyên về các loại hình tội phạm mạng và các cảnh báo về các mối đe dọa an ninh mạng mới (ví dụ: các loại mã độc hoặc lừa đảo mạng đang diễn ra).

Ba là, xây dựng quy định trong tăng cường hợp tác giữa các cơ quan ban ngành phục vụ cho công tác phòng, chống và xử lý tội phạm mạng.

Theo khảo sát về chiến lược an ninh mạng của các quốc gia trong khối OECD, hầu hết các quốc gia đều dựa trên sự hợp tác giữa các bên liên quan để đạt được thành công khi triển khai chiến lược an ninh mạng. Tuy nhiên, cơ chế hợp tác này rất khác nhau giữa các quốc gia. Ví dụ: ở Đan Mạch, cơ quan số hóa (thuộc Bộ Tài chính) và Trung tâm An ninh mạng (Bộ Quốc phòng) cùng phối hợp để quản lý an ninh mạng quốc gia. Vai trò này lại trực thuộc chỉ riêng Bộ Tư pháp ở Hà Lan. Ở các quốc gia như Hoa Kỳ, Latvia và Tây Ban Nha, Hội đồng an ninh mạng quốc gia phụ trách nhiệm vụ này; được thành lập trên cơ sở tập hợp đại diện của tất cả các bộ, ngành liên quan. Còn ở Việt Nam, Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông phối hợp trong công tác phòng, chống tội phạm mạng. Tuy nhiên, để đạt được hiệu quả thì sự phối hợp này cần phải có sự chung tay của cả hệ thống chính trị, mà nòng cốt là các cơ quan chuyên trách an ninh mạng ở tất cả các bộ ngành liên quan và cả các doanh nghiệp cung cấp dịch vụ an ninh mạng và trường đại học-nơi chuyên nghiên cứu về các giải pháp an ninh mạng.

Bốn là, ưu tiên trong xây dựng cơ chế phối hợp trong đào tạo và tuyển dụng đội ngũ chuyên gia về quản trị rủi ro an ninh mạng.

Tương tự như các nước khác, Chính phủ Việt nam cần xây dựng các chính sách ưu tiên trong đào tạo và tuyển dụng đội ngũ nhân lực về quản lý rủi ro an ninh mạng. Các chính sách này nên có sự phối hợp giữa các cơ sở giáo dục đào tạo hoặc viện nghiên cứu các bộ ban ngành. Ví dụ như ở Mỹ, Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST), thuộc Bộ Thương mại, khởi động một chương trình quốc gia về Giáo dục An ninh Mạng (NICE). Chương trình này có sự hợp tác giữa Chính phủ, trường đại học và doanh nghiệp để giúp giảm thiểu khoảng cách về trình độ của lực lượng lao động làm việc trong lĩnh vực an ninh mạng. Hoặc một trong những chương trình hành động mà Chính phủ Canada thực hiện nhằm khắc phục tình trạng thiếu hụt lực lượng lao động trong lĩnh vực an ninh mạng trong tương lai là phát triển các chương trình giáo dục dạy các kĩ năng lập trình và số hoá cho trẻ em từ khi các em còn rất nhỏ.

Năm là, xây dựng các chính sách nhằm khuyến khích tạo ra hệ thống sinh thái sáng tạo trong lĩnh vực an ninh mạng.

Chính phủ đóng vai trò quan trọng trong tạo ra hệ sinh thái khởi nghiệp sáng tạo trong lĩnh vực CNTT và an ninh mạng. Bởi vì, điều này sẽ là bước khởi đầu cho sự phát triển những ý tưởng đột phá trong lĩnh vực này. Gần đây ngày càng nhiều quốc gia triển khai các chính sách khuyến khích giải pháp sáng tạo trong an ninh mạng. Hành động cụ thể chính là thành lập các trung tâm khởi nghiệp sáng tạo trong lĩnh vực bảo mật và an ninh mạng để thực hiện tài trợ cho các dự án nghiên cứu và phát triển các sản phẩm có tính đột phá trong lĩnh vực an toàn và an ninh mạng. Điển hình như Úc thành lập Hiệp hội phát triển an ninh mạng vào năm 2017 hay Anh ra mắt Trung tâm về các tiến bộ công nghệ an ninh mạng vào năm 2018. Hay Đức thành lập Cơ quan Đổi mới Sáng tạo về An ninh Mạng vào năm 2018. Tại Châu Á, Singapore là quốc gia đi tiên phong trong lĩnh vực này với sự ra đời của Hệ sinh thái an ninh mạng sáng tạo (ICE71) vào năm 2018. ICE71 chính là sự hợp tác giữa Singtel Innov8 (chi nhánh đầu tư mạo hiểm của Tập đoàn Singtel) và Đại học Quốc gia Singapore (NUS). ICE71 có các chương trình hỗ trợ cho các công ty khởi nghiệp ở lĩnh vực an ninh mạng từ giai đoạn "ý tưởng" đến giai đoạn "phát triển" và "mở rộng quy mô". ICE71 cũng được hỗ trợ rất lớn bởi Cơ quan An ninh Mạng của Singapore và Bộ Thông tin-Truyền thông. Kể từ khi ra mắt cho đến nay, hệ sinh thái này đã hỗ trợ cho hơn 70 công ty khởi nghiệp trong lĩnh vực an ninh mạng (OECD, 2020).

6.2. Kiến nghị với Ngân hàng Nhà nước

Thứ nhất, Ngân hàng nhà nước (NHNN) cần đảm bảo sự đồng bộ và phù hợp của các quy định pháp lý hiện hành về giao dịch điện tử, chữ ký, chứng từ điện tử, việc định danh và xác thực khách hàng điện tử, việc chia sẻ dữ liệu và bảo mật thông tin khách hàng, quy trình nghiệp vụ... với thực tiễn ứng dụng công nghệ số trong hoạt động ngân hàng.

Thứ hai, NHNN cần tạo ra cơ chế cho phép có sự kết nối liên thông, tích hợp liền mạch giữa các ngân hàng với nhau và hơn nữa là giữa các ngân hàng với các cơ quan chức năng như Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng và các tổ chức cung cấp dịch vụ hạ tầng CNTT để hình thành hệ sinh thái số và qua đó hỗ trợ hoạt động đảm bảo an toàn, an ninh mạng của ngành Ngân hàng. Về dữ liệu, NHNN cũng nên phối hợp với các cơ quan chức năng để cần sớm hoàn thành việc xây dựng cơ sở dữ liệu quốc gia về dân cư; có cơ chế cho phép ngành ngân hàng được kết nối và khai thác, chia sẻ thông tin trực tuyến từ cơ sở dữ liệu này

để phục vụ việc đối chiếu, xác minh định danh khách hàng bằng phương thức điện tử.

Thứ ba, NHNN cần tập trung kiện toàn khung pháp lý cho hoạt động ngân hàng số. Trước tiên, NHNN cần đẩy nhanh tiến độ nghiên cứu xây dựng Luật Giao dịch điện tử thay thế hoặc sửa đổi, bổ sung Luật Giao dịch điện tử năm 2005 để tạo cơ sở pháp lý cho các bộ, ngành hoàn thiện các quy định pháp luật có liên quan, giúp đẩy mạnh số hóa, ứng dụng kỹ thuật số, tạo môi trường giao dịch thuận lợi cho người dân, doanh nghiệp qua kênh số, phương thức điện tử. Sau đó, NHNN cũng nên sớm ban hành Nghị định về định danh và xác thực điện tử và xây dựng hành lang pháp lý về bảo vệ dữ liệu, bảo vệ quyền riêng tư dữ liệu người dùng trên môi trường mạng. Trong tương lai, NHNN cũng sớm nghiên cứu xây dựng luật cho phép thành lập loại hình ngân hàng kinh doanh theo hướng ngân hàng số toàn diện.

Thứ tư, NHNN cần nghiên cứu, áp dụng các tiêu chuẩn, thông lệ quốc tế về an ninh, an toàn hệ thống CNTT vào các văn bản quy phạm pháp luật điều chỉnh hoạt động ứng dụng CNTT của các ngân hàng và tổ chức tín dụng (TCTD) có phát triển ngân hàng số. Cần sớm đưa vào áp dụng khung đánh giá rủi ro CNTT theo thông lệ quốc tế để nâng cao chất lượng công tác thanh tra, kiểm tra tuân thủ các quy định về an toàn bảo mật tại các ngân hàng và TCTD.

Thứ năm, NHNN cần giám sát, đôn đốc các ngân hàng và TCTD hoàn thành triển khai các giải pháp về an toàn an ninh mạng trong đó tập trung kiện toàn bộ máy chuyên trách về an ninh thông tin (ANTT). Tiếp tục đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố an ninh CNTT ngành Ngân hàng.

Thứ sáu, NHNN cần tiếp tục đẩy mạnh công tác truyền thông, nâng cao nhận thức cho cán bộ, nhân viên trong ngành Ngân hàng và cả người dân trong việc nhận diện và giảm thiểu các rủi ro an ninh mạng. Qua đó, có các biện pháp chủ động phòng vệ với các hình thức tấn công mạng ngày càng tinh vi của tội phạm mạng ngày nay.

6.3. Giải pháp hạn chế rủi ro an ninh mạng đối với NH chuyển đổi số

Rủi ro an ninh mạng là vấn đề trung tâm trong hoạt động ngân hàng số. Để giảm thiểu rủi ro an ninh mạng, chúng tôi đề xuất các nhóm giải pháp xoay quanh 3 trụ cột chính: Quy trình (Process), Công nghệ (Technology) và Con người (People). Cụ thể, nhóm giải pháp về quy trình

sẽ tập trung vào việc loại bỏ các quy trình thủ công có thể dẫn đến sai lầm trong thực tiễn quản lý rủi ro an ninh mạng, giới thiệu quy trình chi tiết các bước trong quản trị rủi ro an ninh mạng đặc biệt là các tình huống sử dụng để ứng phó sự cố. Trong khi đó, nhóm giải pháp công nghệ sẽ xây dựng trên cơ sở kết hợp các công cụ và kỹ thuật bảo mật hiện đại và tốt nhất. Cuối cùng là nhóm giải pháp về nhân sự sẽ tiếp cận theo hướng xây dựng văn hóa nhận thức về an ninh mạng. Dưới đây là chi tiết về các nhóm giải pháp xoay quanh các trụ cột chính ấy.

6.3.1. Nhóm giải pháp về quy trình quản trị rủi ro an ninh mạng

Rủi ro an ninh mạng là mối đe dọa hàng đầu của các ngân hàng và định chế tài chính đặc biệt là ngân hàng số. Quản trị rủi ro an ninh mạng là quá trình xác định, phân tích, đánh giá và giải quyết các mối đe dọa an ninh mạng của các ngân hàng. Để hạn chế rủi ro an ninh mạng, việc thiết lập quy trình quản trị rủi ro an ninh mạng là rất cần thiết, đồng thời ngân hàng cần có biện pháp giám sát hiệu quả việc tuân thủ chặt chẽ quy trình của các nhân viên.

Theo báo cáo của Deloitte về Quản trị rủi ro an ninh mạng toàn cầu, chỉ 42% người tham gia cuộc khảo sát cho rằng tổ chức của họ "cực kỳ hiệu quả" hoặc "rất hiệu quả" trong việc quản trị rủi ro mạng (Apcert, 2020). Để quản trị rủi ro an ninh mạng, các ngân hàng chủ yếu sử dụng các chiến lược ngăn chặn rủi ro (blocking and tackling strategies) để khóa các thiết bị, hệ thống và nền tảng của mình từ xa khi có nguy cơ đe doạ an ninh mạng của ngân hàng (Friedman, 2016). Bên cạnh đó, báo cáo này cũng chỉ ra một số vấn đề chung mà ngân hàng và các định chế tài chính gặp phải trong quản trị rủi ro an ninh mạng, bao gồm:

- Ngân sách an ninh mạng tăng lên đáng kể trong vài năm qua. Tuy nhiên, tốc độ gia tăng như vậy sẽ không bền vững trong thời gian dài. Như vậy, định chế tài chính cần phải đưa ra mức độ ưu tiên cho các vấn đề cần xử lý. Điều này không dễ dàng đối với các giám đốc an ninh thông tin (CISO).
- Các CISO bị mắc kẹt trong việc quyết định các lựa chọn ưu tiên. Họ gặp nhiều khó khăn trong việc giải quyết các lỗ hổng trong rất nhiều hệ thống cũ. Họ được kỳ vọng sẽ đổi mới công ty thông qua điện toán đám mây, FinTech, nhận dạng kỹ thuật số và các đột phá công nghệ mới, ngay cả khi họ đang phải nỗ lực cố gắng để các hệ thống lõi của tổ chức được duy trì và hoạt động. Cùng lúc đó, họ phải điều chỉnh

các chính sách và nỗ lực an ninh mạng với các chiến lược kinh doanh, hoạt động và công nghệ của định chế tài chính.

- Các CISO gặp khó khăn trong việc đánh giá và tích hợp một loạt các công cụ bảo mật mới, đồng thời đổi mới tổ chức của họ để đưa an ninh mạng trở thành yếu tố cốt lõi trong toàn doanh nghiệp.
- Thiếu hụt nhân sự tài năng trong lĩnh vực quản trị an ninh mạng là một thách thức lớn mà các định chế tài chính hiện đối mặt.
- Thiếu các tiêu chuẩn đo lường rủi ro mạng quốc tế và các tiêu chuẩn trong toàn ngành để đáp ứng nhu cầu giám sát ngày càng tăng.
- CISO cần trợ giúp để "connecting the dots". Sự mơ hồ về pháp lý hoặc các rào cản quy định là những trở ngại đối với việc chia sẻ thông tin trong và ngoài ngành, và thậm chí cả trong nước sở tại của họ.

Hiện nay, Việt Nam ban hành một số quy định về kiểm soát rủi ro an ninh mạng cho hệ thống ngân hàng phù hợp với quy định tiêu chuẩn quốc tế về quản lý an ninh thông tin *(ISO/IEC 27001:2013)*. Tuy nhiên, ở nhiều nước phát triển như Mỹ, Anh, các nước liên minh Châu Âu hiện đang áp dụng đồng bộ một số tiêu chuẩn và khuôn khổ pháp lý quy định về cách thức quản trị rủi ro an ninh mạng cho hệ thống ngân hàng, bao gồm:

- ISO/IEC 27001:2013 quy định tiêu chuẩn quốc tế về quản lý an ninh thông tin.

  Kiểm soát CIS (Trung tâm An ninh Internet) gồm một tập hợp 20 biện pháp kiểm soát bảo mật được đề xuất để phòng thủ mạng, cung cấp các cách thức cụ thể và khả thi để ngăn chặn các cuộc tấn công phổ biến và nguy hiểm nhất hiện nay. Bộ Ngoại giao Hoa Kỳ tuyên bố đã giảm được 94% rủi ro "được đo lường" thông qua việc áp dụng nghiêm ngặt các biện pháp kiểm soát này. 20 biện pháp kiểm soát của CIS đều được thể hiện trong các kiểm soát của Phụ lục A của ISO27001, vì vậy CIS được tích hợp liền mạch với ISO27001. Tuy nhiên, CIS cung cấp các hướng dẫn triển khai, tự động hóa, đo lường và kiểm tra/đánh giá chi tiết những biện pháp hiệu quả nhất để giảm thiểu các cuộc tấn công mạng. Các biện pháp được thiết kế phải là những biện pháp nhận được sự đồng thuận của nhiều chuyên gia bảo mật. Như vậy, chúng tôi đề xuất Chính phủ

và NHNN và cả các NHTM nên hoàn thiện cơ sở pháp lý về quản trị rủi ro an ninh mạng dựa trên kiểm soát CIS[121].

- PCI DSS (Tiêu chuẩn Bảo mật dữ liệu thẻ thanh toán) - áp dụng cho các tổ chức chấp nhận thanh toán bằng thẻ. Để bảo vệ dữ liệu chủ thẻ, công ty phải tuân thủ tất cả các yêu cầu bảo mật dữ liệu PCI DSS.

Mặc dù có nhiều phương pháp khác nhau, chúng tôi đề xuất quy trình quản trị rủi ro an ninh mạng tuân theo các bước sau:

Bước 1. Xác định rủi ro. Việc xác định rủi ro có thể ảnh hưởng đến an ninh mạng của ngân hàng thường liên quan đến việc xác định các lỗ hổng bảo mật mạng trong hệ thống và các mối đe dọa có thể khai thác chúng. Do an ninh mạng là một lĩnh vực không ngừng phát triển cho nên việc xác định và phân loại rủi ro sẽ là mục tiêu động. Đây được xem là một trong những thách thức lớn nhất của các nhà quản trị ngân hàng cũng như các giám đốc an ninh thông tin (CISCO). Các bước xác định rủi ro an ninh mạng thường được áp dụng bao gồm:

- Xác định tài sản cần được bảo vệ. Ngân hàng phải xác định rõ các tài sản (thông tin, dữ liệu) cần được bảo vệ và mức độ ưu tiên của chúng.
- Xác định các mối đe dọa đối với tài sản của ngân hàng. Phân tích mối đe dọa liên quan đến việc xác định trường hợp hoặc sự kiện có khả năng ảnh hưởng tiêu cực đến hoạt động hoặc tài sản thông qua việc truy cập trái phép hệ thống thông tin, cũng như xác định các nguồn có thể gây hại cho tài sản. Nhà phân tích cần phân biệt các mối đe dọa liên quan hay không liên quan đến an ninh mạng. Các mối đe dọa có thể từ lỗi kỹ thuật (lỗi cấu trúc hoặc cấu hình), lỗi của con người (từ nội bộ, từ các đối tác của ngân hàng) hoặc các cuộc tấn công thù địch từ bên ngoài. Để xác định thành công các mối đe dọa đòi hỏi kinh nghiệm của các nhà phân tích chuyên nghiệp.
- Xác định các lỗ hổng trước những mối đe dọa đó. Trong bước này, nhà phân tích cần xác định các điểm yếu của ngân hàng trong môi trường an ninh mạng có thể khiến ngân hàng dễ bị tổn thương trước những mối đe dọa đó. Chẳng hạn, các điểm yếu trong hệ thống

[121] *Chi tiết về các biện pháp kiểm soát bảo mật được trình bày ở Phụ lục 1*

thông tin, quy trình bảo mật, kiểm soát nội bộ hoặc việc thực hiện có thể bị khai thác bởi các mối đe dọa đã được xác định trước đó.

Bước 2. Phân tích mức độ tác động của từng rủi ro. Đây là bước được thực hiện thông qua đánh giá khả năng xảy ra và mức độ ảnh hưởng (ước tính hậu quả tiềm ẩn và tác động chi phí của nó). Đây là thông tin quan trọng để nhà quản trị đưa ra các quyết định quản trị rủi ro và các biện pháp ứng phó rủi ro trong tương lai. Nhà phân tích cần liệt kê các rủi ro theo khả năng xảy ra và tác động của nó để xác định rủi ro tổng thể. Nhà phân tích cần làm rõ mục đích, phạm vi, các ràng buộc và mô hình phân tích rủi ro sẽ được sử dụng.

Bước 3. Đánh giá rủi ro. Đánh giá rủi ro là bước cần phân tích xem mỗi rủi ro có nằm trong mức rủi ro mà ngân hàng chấp nhận được hay không. Nhà phân tích mô tả mức độ ưa thích liên quan đến từng rủi ro và cơ hội, mức độ hành động cần thiết và mức độ tác động có thể chấp nhận được. Việc thiết lập trước mức độ rủi ro chấp nhận được sẽ giúp ngân hàng tập trung vào thái độ và hành động cần thiết đối với rủi ro mạng để đáp ứng kỳ vọng của Hội đồng quản trị.

Bước 4. Ưu tiên các rủi ro. Ưu tiên rủi ro có thể được áp dụng cho từng rủi ro để làm cơ sở cho mức độ rủi ro chung trên không gian mạng. Việc xác định và ưu tiên các rủi ro an ninh mạng để ngân hàng có thể phân bổ nguồn lực một cách khôn ngoan để cải thiện an toàn không gian mạng. Nhà phân tích có thể dùng phương pháp định tính hoặc định lượng. Các phương pháp định tính đánh giá rủi ro dựa trên các danh mục hoặc mức độ như thấp, trung bình và cao. Các phương pháp định lượng liên quan đến việc xác định các giá trị cho khả năng xảy ra rủi ro và tổn thất dựa trên ma trận.

Bước 5. Quyết định cách ứng phó với từng rủi ro. Thông thường có bốn lựa chọn:

- Lựa chọn 1. Xử lý - sửa đổi khả năng xảy ra và / hoặc tác động của rủi ro, thường bằng cách thực hiện các biện pháp kiểm soát an ninh.
- Lựa chọn 2. Chịu đựng - đưa ra quyết định chủ động để giữ lại rủi ro (ví dụ: vì nó nằm trong các tiêu chí chấp nhận rủi ro đã thiết lập).
- Lựa chọn 3. Chấm dứt - tránh hoàn toàn rủi ro bằng cách chấm dứt hoặc thay đổi hoàn toàn hoạt động gây ra rủi ro.
- Lựa chọn 4. Chuyển giao - chia sẻ rủi ro với một bên khác, thường bằng cách thuê ngoài hoặc mua bảo hiểm.

Các biện pháp giảm thiểu rủi ro công nghệ bao gồm mã hóa, tường lửa, phần mềm săn tìm mối đe dọa và tự động hóa tương tác để tăng hiệu quả hệ thống. Các phương pháp hay nhất để giảm thiểu rủi ro bao gồm các chương trình đào tạo về an ninh mạng, cập nhật phần mềm, các giải pháp quản lý truy cập đặc quyền (PAM), xác thực truy cập đa yếu tố và sao lưu dữ liệu động.

Bước 6. Liên tục giám sát rủi ro. Đây là bước nhằm đảm bảo các rủi ro vẫn có thể chấp nhận được, xem xét các biện pháp kiểm soát của bạn để đảm bảo chúng vẫn phù hợp với mục đích và thực hiện các thay đổi theo yêu cầu. Rủi ro liên tục thay đổi khi bối cảnh mối đe dọa mạng phát triển, đồng thời các hệ thống và hoạt động của ngân hàng cũng thay đổi.

6.3.2. Nhóm giải pháp về công nghệ

Bên cạnh việc xây dựng quy trình quản trị rủi ro an ninh mạng hiệu quả, công nghệ là yếu tố rất quan trọng quyết định việc ngân hàng có bảo đảm an toàn an ninh mạng thành công và hiệu quả hay không. Sử dụng các công nghệ tiên tiến giúp các ngân hàng thực hiện quy trình và giám sát việc tuân thủ quy trình một cách hiệu quả và chặt chẽ hơn. Các công nghệ giúp các tổ chức giảm thời gian để xác định hay phát hiện rủi ro an ninh mạng và giảm thời gian để phản ứng với các sự cố. Các sự cố có thể được phát hiện một cách chính xác và được khắc phục chỉ trong vài phút, thay vì vài ngày, vài tuần hoặc lâu hơn. Công nghệ cũng cho phép bộ phận an ninh tự động hóa các quy trình ứng phó các sự cố an ninh mạng. Một số công nghệ thông minh như công nghệ trí tuệ nhân tạo (Artificial Intelligence - AI) còn có thể cải thiện Tri thức an ninh mạng (Threat Intelligence - TI)[122], cải thiện khả năng dự đoán nguy cơ và bảo đảm an ninh mạng. Trí tuệ nhân tạo có thể học hỏi từ các nhà phân tích bảo mật và cải thiện hiệu quả của nó theo thời gian, điều này giúp tiết kiệm thời gian và đưa ra quyết định tốt hơn. Điều này rất cần thiết cho các ngân hàng khi các cuộc tấn công mạng tiếp tục phát triển về số lượng và mức độ tinh vi. Với sự trợ giúp hiệu quả và chính xác từ công nghệ thông minh, ngân hàng giảm áp lực nhu cầu về các chuyên gia an ninh mạng, giảm áp lực do thiếu hụt nguồn cung nghiêm

---

[122] *Tri thức an ninh mạng (Threat Intelligence - TI) là một cách tiếp cận mới đối với việc ngăn chặn các mối đe dọa trên không gian mạng. TI ra đời nhằm giúp cung cấp nguồn dữ liệu lớn về các mối đe dọa trên không gian mạng, giúp cho các Tổ chức chủ động phát hiện các mối nguy hại an ninh mạng từ sớm và qua đó có các biện pháp phòng chống, giúp nâng cao hiệu quả, giảm thiểu ảnh hưởng đến hoạt động kinh doanh.*

trọng về chuyên gia an ninh mạng trong thời gian gần đây. Tuy nhiên, đầu tư vào công nghệ tiên tiến đòi hỏi ngân hàng phải dành một khoản ngân sách rất lớn và đầu tư bảo mật một cách đồng bộ. Vì vậy, các ngân hàng cần quyết định lựa chọn công nghệ tiên tiến và hiệu quả để đảm bảo an toàn an ninh mạng cho mình.

Theo khảo sát của Accenture Security (2020) cho 4,644 giám đốc điều hành của các tổ chức có doanh thu hàng năm trên 1 tỷ USD từ 24 ngành công nghiệp và 16 quốc gia ở Bắc Mỹ, Nam Mỹ, châu Âu và châu Á - Thái Bình Dương, các giám đốc điều hành cho rằng ba thước đo đo lường sự thành công của chương trình an ninh mạng là:

- Tốc độ phát hiện sự cố mạng (mất bao lâu để phát hiện sự cố và độ chính xác trong việc tìm kiếm các sự cố mạng)
- Thời gian phục hồi mạng (có bao nhiêu hệ thống đã bị dừng và mất bao lâu để hệ thống khôi phục hoạt động bình thường)
- Thời gian phản hồi mạng (mất bao lâu để xác định và phản hồi)

Đây cũng là các thước đo quyết định ưu tiên lựa chọn công nghệ của các nhà lãnh đạo của các công ty lớn trong việc đầu tư bảo đảm an ninh mạng.

Hiện nay, các công nghệ tiên tiến được sử dụng để đảm bảo an toàn an ninh mạng trên thế giới, bao gồm:

- *Trí tuệ nhân tạo (Artificial Intelligence - AI)*: mô phỏng trí thông minh của con người bằng cách lập trình máy móc để chúng có thể có suy nghĩ và hành động giống như con người hoặc bắt chước hành động của họ.
- *Công nghệ tự động hóa, phản hồi, điều phối và bảo mật (Security, Orchestration, Automation, Response - SOAR)*: cho phép sắp xếp hợp lý các hoạt động bảo mật trong ba lĩnh vực chính: quản lý mối đe dọa và lỗ hổng bảo mật, ứng phó sự cố, và tự động hóa các hoạt động bảo mật.
- *Chứng thực rủi ro cơ sở (Risk-based authentication – RBA):* phương pháp cải thiện bảo mật tài khoản trên các trang web. RBA áp dụng các mức độ nghiêm ngặt khác nhau cho các quy trình xác thực dựa trên khả năng truy cập vào một hệ thống nhất định có thể dẫn đến việc nó bị xâm phạm.

- *Công nghệ tường lửa thế hệ tiếp theo (Next-Generation Firewall – NGF)*: thiết bị bảo mật mạng cung cấp các khả năng vượt trội so với công nghệ tường lửa truyền thống. Tường lửa truyền thống thường cung cấp khả năng kiểm tra trạng thái lưu lượng mạng đến và đi, trong khi tường lửa thế hệ tiếp theo còn bổ sung thêm các tính năng như nhận thức và kiểm soát ứng dụng, ngăn chặn xâm nhập tích hợp và thông minh về mối đe dọa do hệ thống đám mây cung cấp.
- *Tự động hóa qui trình bằng rô bốt (Robotic Process Automation – RPA):* công nghệ phần mềm giúp dễ dàng xây dựng, triển khai và quản lý rô bốt bằng phần mềm để mô phỏng các hành động của con người tương tác với các hệ thống và phần mềm kỹ thuật số. Ví dụ, Adhikari (2021) cho rằng khi RPA được triển khai, hệ thống an ninh mạng có thể hoạt động một cách liên tục và đặc biệt hệ thống phòng vệ sẽ được kích hoạt một cách tự động mà không cần đến sự can thiệp của con người. Các phần mềm dựa trên RPA sẽ tự động rà soát hạ tầng mạng, từ đó đưa ra được các giải pháp kiểm soát, phòng ngừa một cách hiệu quả.
- *Quản lý quyền truy cập đặc quyền (Privileged Access Management – PAM)*: hệ thống quản lý an toàn tài khoản của những người có quyền truy cập đặc quyền. Tài khoản của họ là mục tiêu thường nhắm tới của tội phạm mạng.

Báo cáo gần đây của Accenture Security cho thấy các nhà lãnh đạo thường xếp hạng ưu tiên cho các công nghệ bảo mật khi các công nghệ này đưa vào sử dụng. Kết quả cũng cho thấy mỗi công nghệ đều có thế mạnh nhất định tuỳ theo khía cạnh ưu tiên mà doanh nghiệp đặt ra trong chính sách về an ninh mạng (bảng 4).

Bảng 4: Xếp hạng ưu tiên các công nghệ bảo mật cho an ninh mạng

Ưu tiên	SOAR	AI	NGF	RBA	RPA	PAM
Phát hiện sự cố nhanh hơn	#2	#1	#3	#4		
Phản ứng sự cố nhanh hơn	#1	#1		#4	#3	

Thời gian phục hồi ngắn hơn	#1	#2		#3	#4	

Nguồn: Accenture Security (2020)

Bên cạnh đó, Accenture Security cũng đưa ra bảng xếp hạng công nghệ theo lợi ích mà các công ty thu được khi sử dụng như tính chính xác trong phát hiện sự cố, chi phí tối ưu, chất lượng phản hồi hay ít cuộc tấn công thành công hơn (bảng 5).

Bảng 5: Xếp hạng lợi ích của công nghệ đối với an ninh mạng

Lợi ích của công nghệ	SOAR	AI	NGF	RBA	RPA	PAM
Ít cuộc tấn công thành công hơn	#2		#1	#4		#3
Mức độ thiệt hại thấp khi có xảy ra tấn công mạng	#3	#1	#2			#4
Phát hiện sự cố chính xác hơn	#1	#2	#3		#4	
Giảm rủi ro vốn có/Thu nhỏ phạm vi tấn công	#1		#3	#2		#4
Giảm chi phí	#1	#2		#3	#4	
Chất lượng phản hồi nhất quán	#2	#1		#4	#3	

Nguồn: Accenture Security (2020)

Theo kết quả khảo sát được trình bày ở bảng trên, *trí tuệ nhân tạo (AI) và công nghệ tự động hóa, phản hồi, điều phối và bảo mật (SOAR)* là hai công nghệ quan trọng nhất và được xem là thành công nhất trong chiến lược đầu tư công nghệ đảm bảo an ninh mạng. Điểm lưu ý là một số các công nghệ bảo mật liệt kê ở trên đang được phát triển dựa trên cơ sở nền tảng công nghệ Blockchain; đây cũng là xu hướng công nghệ bảo mật của tương lai. Thật vậy, theo Ed Powers, Trưởng nhóm Rủi ro Mạng của Deloitte tại Hoa Kỳ, *"mặc dù còn khá non trẻ nhưng công nghệ Blockchain là công*

nghệ đầy hứa hẹn trong việc giúp các doanh nghiệp đương đầu với những thách thức ngày càng gia tăng về rủi ro mạng đặc biệt ở tính định danh kỹ thuật số (digital identity) và sự toàn vẹn của dữ liệu (data integrity) khi sử dụng công nghệ" (Deloitte, 2017).

Về bản chất, công nghệ Blockchain là công nghệ cho phép dữ liệu được lưu trữ trong nhiều khối (blocks) và phân tán ở các máy chủ khác nhau. Dữ liệu lưu trên các khối sẽ được làm mới định kỳ với tần suất được thiết lập trước. Các giao dịch liên quan đến công nghệ này đều tồn tại ở dạng kĩ thuật số, và dữ liệu vì thế hầu như không thể bị thay đổi. Tất cả giao dịch và dữ liệu sẽ không bị ảnh hưởng bởi vì ngay cả khi các hackers xâm nhập vào được một khối, dữ liệu trên các khối khác vẫn sẽ được bảo vệ bằng mã hóa, kĩ thuật số. Do đó, công nghệ Blockchain sẽ giúp các tổ chức tài chính giảm thiểu rủi ro an ninh mạng cũng như giúp phát hiện, ngăn chặn và chống lại các đe doạ an ninh mạng.

Tuy nhiên, công nghệ blockchain vẫn chưa phải là một công nghệ hoàn hảo khi mà công nghệ này có cả ưu và nhược điểm tồn tại song song. Ví dụ, công nghệ Blockchain có những tính năng nổi trội như: cấu trúc phân tán, cơ chế xác nhận đồng thuận, dữ liệu được mã hóa, tính minh bạch. Mặt khác, công nghệ Blockchain lại chứa đựng nhiều rủi ro tiềm ẩn như lỗi mã hóa của các phần mềm sử dụng, rủi ro từ nguồn dữ liệu ngoài, danh tính người dùng có thể bị giả mạo, và cả những hình thức tấn công tiềm tàng mới[123].

Vì thế, các tổ chức tài chính khi áp dụng công nghệ Blockchain vào hệ thống an ninh mạng cần xem xét và cân nhắc thật kỹ lưỡng để nhằm hạn chế hạn chế rủi ro có thể phát sinh do sử dụng công nghệ này. Hơn nữa, các nhà lãnh đạo ngân hàng cũng nên có sự lựa chọn và tập trung nguồn lực đầu tư vào các công nghệ nào mang lại giá trị cao, phù hợp với mục tiêu ngân hàng đề ra cũng như nguồn lực tài chính của mình.

6.3.3. Nhóm giải pháp về con người

Theo phát biểu của Yi Fang Chua, Giám đốc cấp cao về an ninh mạng của Earnt & Young, con người chính là mắt xích yếu nhất của một tổ chức trong 3 trụ cột (Con người, Quy trình và Công nghệ). Bởi vì "*cho dù tổ chức có bất kể công nghệ tiên tiến và quy trình bảo mật chặt chẽ như thế*

[123] *Xem thêm chi tiết ở Phụ lục 2*

nào đi chăng nữa thì an ninh mạng của tổ chức sẽ luôn bị đe dọa bởi chính những con người làm việc trong tổ chức đó". Vì thế, để hạn chế nguy cơ này, chúng tôi đề xuất các ngân hàng nên thực hiện các giải pháp sau đây:

Thứ nhất, thiết kế chương trình đào tạo an ninh mạng cho nhân viên

Đào tạo toàn diện về nhận thức bảo mật an ninh mạng cho nhân viên cũng như các đối tác là một trong những cách tốt nhất để bảo vệ ngân hàng khỏi các tác nhân độc hại và ngăn chặn các vi phạm có thể xảy ra. Nhân viên ngân hàng thường là tuyến phòng thủ đầu tiên chống lại sự đe dọa an ninh mạng.

Nhân viên ngân hàng cần tham gia các khóa đào tạo để nâng cao nhận thức về bảo mật, hiểu các lỗ hổng, nhận ra các mối đe dọa mạng phổ biến và các mối đe dọa đối với hoạt động kinh doanh cũng như lý do họ nên quan tâm đến an ninh mạng. Nhân viên cần nắm vững các thủ tục và chính sách an ninh mạng của ngân hàng, nhận thức rõ vai trò và trách nhiệm đối với an ninh mạng của họ. Nhân viên cần nhận thức rõ trách nhiệm và trách nhiệm giải trình của họ khi sử dụng máy tính trong mạng lưới kinh doanh. Các khóa đào tạo bồi dưỡng nên được tổ chức thường xuyên theo lịch trình để nhân viên thấm nhuần văn hóa bảo mật dữ liệu của ngân hàng. Chương trình đào tạo an ninh mạng nên đảm bảo các nội dung sau đây:

(1) *Trách nhiệm về dữ liệu ngân hàng*: Liên tục nhấn mạnh bản chất quan trọng của bảo mật dữ liệu và trách nhiệm của mỗi nhân viên trong việc bảo vệ dữ liệu của ngân hàng và khách hàng. Luôn gắn nhân viên với các quy định và nghĩa vụ pháp lý trong tôn trọng và bảo vệ quyền riêng tư của thông tin cũng như tính toàn vẹn và bí mật của thông tin.

(2) *Các thủ tục quản lý tài liệu và thông báo*: đào tạo cho nhân viên cách nhận ra một thông báo hoặc cảnh báo hợp pháp, các quy trình báo cáo sự cố dữ liệu, nhân viên cần nhận thức việc báo cáo ngay sự cố để ngân hàng xử lý kịp thời nhằm giảm thiểu thiệt hại từ sự cố.

(3) *Mật khẩu:* đào tạo về cách chọn mật khẩu mạnh: khó đoán nhưng phải dễ nhớ. Hệ thống thiết lập lời nhắc tự động định kỳ yêu cầu nhân viên thay đổi mật khẩu.

(4) *Phần mềm trái phép:* không được phép tải xuống phần mềm không được cấp phép hay cài đặt phần mềm trái phép trên máy tính của ngân hàng.

(5) *Sử dụng Internet:* nhân viên cần tránh các liên kết được gửi qua email hoặc được gửi trực tuyến (online) đáng ngờ hoặc từ các nguồn không xác định. Ngân hàng nên thiết lập các quy tắc duyệt web an toàn và các giới hạn về việc sử dụng mạng của nhân viên tại nơi làm việc.

(6) *Email:* để ngăn chặn việc đánh cắp dữ liệu, nhân viên cần biết đề phòng những trò gian lận và không trả lời email không rõ nguồn gốc hay người gửi, những email với nội dung lạ có với cách viết hoặc ký tự bất thường.

(7) T*ấn công phi kỹ thuật và lừa đảo (Social Engineering và Phishing)*: Đào tạo nhân viên nhận ra các rủi ro an ninh thông tin và tội phạm mạng phổ biến như các cuộc tấn công phi kỹ thuật, gian lận trực tuyến, lừa đảo và rủi ro duyệt web.

(8) *Chính sách truyền thông xã hội*: ngân hàng cần có các chính sách và hướng dẫn cụ thể về việc sử dụng địa chỉ email của ngân hàng để đăng ký, đăng (post) hoặc nhận thông qua các phương tiện truyền thông.

(9) *Thiết bị di động*: ngân hàng cần thông báo cho nhân viên về chính sách thiết bị di động bao gồm các thiết bị thuộc sở hữu của công ty và thuộc sở hữu cá nhân được sử dụng trong quá trình kinh doanh.

(10) *Tài nguyên máy tính*: nhân viên phải thường xuyên sao lưu các thông tin quan trọng và lưu giữ các bản sao này ở vị trí an toàn. Nhân viên phải có trách nhiệm chấp nhận các bản cập nhật phần mềm chống virus hiện tại trên các máy tính cá nhân (PC) của ngân hàng.

Thứ hai, thực hiện đào tạo an ninh mạng cho khách hàng

Để giúp khách hàng nâng cao nhận thức về an ninh mạng, đề cao cảnh giác và bảo mật thông tin cá nhân của mình, các ngân hàng nên cung cấp đào tạo và giáo dục về an ninh mạng cho khách hàng thông qua nhiều phương pháp khác nhau. Sử dụng nhiều kênh phân phối có thể giúp đảm bảo khách hàng tham gia chương trình đào tạo này trong suốt cả năm. Đào tạo và giáo

dục về an ninh mạng cũng có thể cung cấp cho khách hàng một điểm khởi đầu hoặc các nguồn lực bổ sung để tự xây dựng một nền văn hóa bảo mật. Các kênh đào tạo và giáo dục an ninh mạng cho khách hàng, bao gồm:

(1) Trang web của ngân hàng: đưa ra các chính sách của ngân hàng về xử lý thông tin hoặc tiết lộ sự cố mạng, tin tức hoặc bài báo về an ninh mạng hoặc các liên kết đến đào tạo về an ninh mạng.

(2) Đăng thông tin hoặc tin tức về an ninh mạng trên các kênh truyền thông xã hội của ngân hàng (LinkedIn, Facebook, Instagram, ...).

(3) Cung cấp thông tin an ninh mạng, cung cấp các gợi ý kiểm soát (như tạo mật khẩu mạnh) hoặc cách tự kiểm tra tại thời điểm mở tài khoản.

(4) Nói chuyện trực tiếp với khách hàng về tầm quan trọng của an ninh mạng.

Chính các hoạt động này còn giúp khách hàng nhận biết ngân hàng đang bảo vệ thông tin của mình như thế nào. Trong thời đại công nghệ 4.0, khi an ninh mạng đang trở thành một yếu tố quyết định thì việc công khai và minh bạch về an ninh mạng có thể tạo niềm tin cho khách hàng hiện hữu và thu hút khách hàng mới.

Thứ ba, xây dựng các biện pháp an ninh mạng với các đối tác ngân hàng

Như phân tích ở trên, rủi ro an ninh mạng của ngân hàng có thể xuất phát từ các đối tác của ngân hàng. Các đối tác có thể là nhà cung cấp dịch vụ CNTT, đơn vị liên kết, cộng tác viên, nhà tư vấn... Đây cũng là một trong ba cửa ngõ chính mà tội phạm mạng dùng để tấn công vào ngân hàng. Khi sự cố an ninh mạng xảy ra cho ngân hàng hoặc khách hàng của ngân hàng do lỗi của các đối tác hoặc do sự tấn công của tội phạm mạng vào các đối tác, ngân hàng có thể phải gánh chịu những thiệt hại về mặt tài chính, thiệt hại về uy tín vì các sự cố an ninh mạng dẫn đến dư luận tiêu cực hoặc làm gián đoạn hoạt động của ngân hàng.Vì vậy, ngân hàng cần chú trọng hơn nữa trong việc đánh giá và kiểm soát rủi ro an ninh mạng từ phía các đối tác.

Việc đánh giá và kiểm soát rủi ro từ các đối tác không hề dễ dàng vì các ngân hàng bị giới hạn, thậm chí là không kiểm soát được cách các đối tác bảo mật cơ sở hạ tầng công nghệ, ứng dụng hoặc dữ liệu của họ. Để giảm thiểu rủi ro từ các đối tác, ngân hàng cần thực hiện các công việc sau:

- Tạo và duy trì kho lưu trữ trung tâm cho các mối quan hệ với đối tác. Ngân hàng cần lưu giữ danh mục hoạt động của các đối tác, nắm rõ danh sách các đối tác. Hiểu rõ các đối tác, chúng ta mới có thể đánh giá kỹ lưỡng rủi ro của mỗi mối quan hệ.
- Đánh giá an ninh mạng cho tất cả các đối tác chứ không riêng nhà cung cấp phần mềm. Trong thời đại chuyển đổi số và Internet, hầu hết mọi mối quan hệ với các đối tác đều liên quan đến việc lưu trữ, xử lý hoặc truyền dữ liệu nhạy cảm.
- Thực hiện các biện pháp phòng ngừa an ninh mạng khi kết thúc hợp tác với các đối tác như chấm dứt quyền truy cập của đối tác vào các hệ thống quan trọng, đối tác phải thông báo cho các kênh thích hợp trước khi thông báo chấm dứt hợp đồng.

6.3.4. Chi tiết hướng dẫn phòng ngừa và giảm thiểu rủi ro an ninh mạng cho các ngân hàng số

Để giảm thiểu rủi ro an ninh mạng, chúng tôi đã đề xuất các ngân hàng thương mại, đặc biệt là các ngân hàng đang chuyển đổi số, cần thực hiện rà soát lại 3 trụ cột trong quy trình quản trị rủi ro an ninh mạng tại ngân hàng. Quan trọng hơn, các NHTM cần phải thực hiện đồng bộ các giải pháp đã gợi ý ở phần trên. Ngoài ra, chúng tôi cũng đề xuất các hướng dẫn chi tiết về các phương án phòng vệ để giúp các NHTM ngăn chặn được các cuộc tấn công mạng cũng như là có thể phục hồi được sau khi bị tấn công mạng. Về cơ bản, các phương án này phải đảm bảo rằng các NHTM đã xem xét đến tất cả các mối đe dọa, có kế hoạch ngăn chặn các vi phạm an ninh mạng và có phương án sẵn sàng ứng phó khi các vi phạm an ninh mạng xảy ra. Lưu ý là các phương án này không chỉ đề cập đến yếu tố kỹ thuật của hệ thống thông tin an ninh mạng mà còn đề xuất các nguyên tắc nhằm ngăn chặn và giảm thiểu các cuộc tấn công mạng có thể xảy ra trong tương lai.

Để thực hiện điều này, chúng tôi đề xuất các NHTM thực hiện theo các nguyên tắc ở bảng 6 sau đây:

Bảng 6: Nguyên tắc phòng ngừa và giảm thiểu rủi ro an ninh mạng

Số thứ tự	Nguyên tắc
1	Đừng dựa vào một giải pháp bảo mật duy nhất, mà thay vào đó hãy sử dụng nhiều lớp bảo mật.

2	Dữ liệu nên được sao lưu thường xuyên để hạn chế thiệt hại nếu bị tấn công nhằm vào dữ liệu như thay đổi, phá huỷ hoặc đánh cắp dữ liệu.
3	Phần mềm nên được đổi mới thường xuyên, giúp bảo vệ tối đa hệ thống.
4	Bảo mật bằng sinh trắc học nên được tích hợp vào hệ thống bảo mật.
5	Phản ứng nhanh chóng để giảm thiểu thiệt hại khi bị tấn công mạng.
6	Nâng cao nhận thức của nhân viên và khách hàng về các mối đe dọa an toàn mạng.
7	Thường xuyên rà soát các chiến lược bảo mật của ngân hàng.
8	Có kế hoạch ứng phó với các cuộc tấn công vào hệ thống an ninh mạng của ngân hàng.

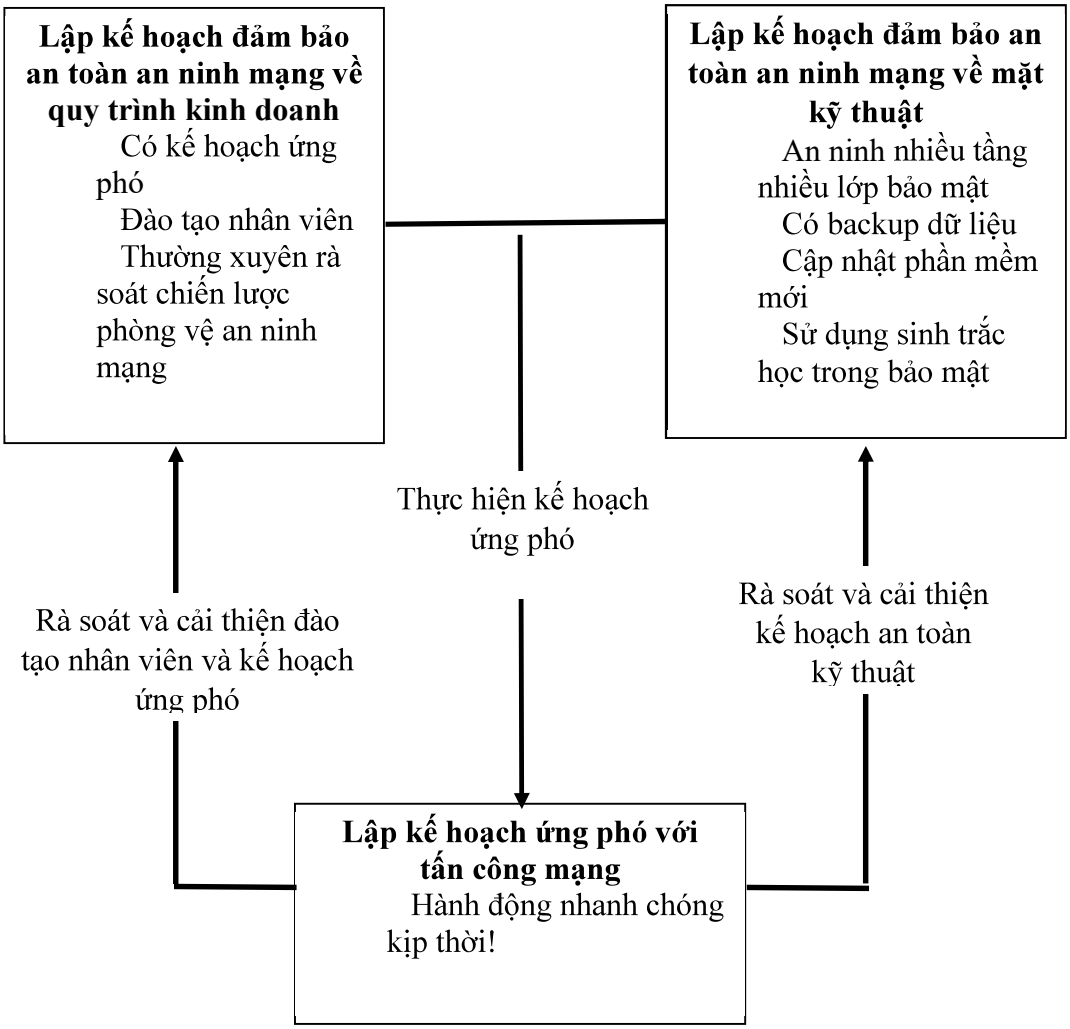
Nguồn: Kay và cộng sự (2021)

Các hướng dẫn trong bảng 6 chỉ mang tính liệt kê và vì thế các NHTM có thể nhóm lại với nhau theo đặc thù của đơn vị mình. Ưu tiên nhất vẫn là *phải có nhiều tầng lớp bảo mật* trong hệ thống CNTT và an ninh mạng (nguyên tắc 1). Bởi vì việc triển khai càng nhiều lớp bảo mật thì ngân hàng sẽ càng ngăn chặn được những đe doạ đến an ninh mạng của ngân hàng. Kế đến, các ngân hàng cũng cần thực hiện *sao lưu dữ liệu* định kỳ để hạn chế thiệt hại khi bị tấn công bởi sâu mạng (nguyên tắc 2). Nếu bị tấn công, ngân hàng khi đó cũng có thể sửa chữa lỗ hổng và thiết lập lại hệ thống một cách nhanh chóng và đặc biệt là ít ảnh hưởng đến hoạt động kinh doanh của ngân hàng. Một nguyên tắc kỹ thuật quan trọng khác là *cập nhật phần mềm thường xuyên* (nguyên tắc 3). Bởi vì không thể có phần mềm nào là hoàn hảo. Do đó, khi các lỗ hổng an ninh mạng được phát hiện hoặc công nghệ bảo mật mới ra đời thì các ngân hàng cũng nên cập nhật kịp thời để khắc phục các vấn đề bảo mật càng sớm càng tốt. *Bảo mật bằng sinh trắc học* cũng nên được tích hợp vào hệ thống của ngân hàng để giúp ngân hàng đảm bảo hệ thống an toàn hơn. Bởi vì hình thức xác thực này ít bị bắt chước hoặc bị đánh cắp hơn (nguyên tắc 4). Lưu ý là tất cả các giải pháp trên đều

thiên về khía cạnh kỹ thuật và tất cả giải pháp đều có vai trò quan trọng đối với sự thành công trong việc ngăn chặn những đe dọa đến an ninh mạng.

Bên cạnh đó, ngân hàng cũng cần thực hiện các giải pháp khác hướng đến việc đảm bảo an toàn trong quy trình hoạt động kinh doanh. Cụ thể, ngân hàng cần phải xây dựng *các kế hoạch ứng phó cho các cuộc tấn công* vào hệ thống an ninh mạng (nguyên tắc 8). Dĩ nhiên ngân hàng sẽ không phải thực hiện các kế hoạch ứng phó này nếu không bị tấn công. Tuy nhiên, một kế hoạch ứng phó không chỉ giúp ngân hàng xác định được các bước để ứng phó khi có sự cố xảy ra mà còn giúp ngân hàng sớm phát hiện các lỗ hổng an ninh mạng. Chính điều này, vì thế, sẽ giúp cho ngân hàng có cơ hội để củng cố các điểm yếu trước khi xảy ra một cuộc tấn công mạng thực sự. Ngoài ra, các ngân hàng cũng nên quan tâm đến việc đào tạo nhân viên về các mối đe dọa an ninh mạng (nguyên tắc 6). Khi đó, có thể giúp ngân hàng ngăn chặn các nguy cơ tấn công mạng bằng phần mềm độc hại và sâu mạng mà nhân viên thường xuyên gặp phải. Các NHTM cũng nên *rà soát liên tục các chiến lược bảo mật* để đảm bảo tính hiệu quả của các chiến lược bảo mật trong việc ngăn chặn các cuộc tấn công mạng (nguyên tắc 7). Bởi vì việc rà soát này không chỉ tập trung ở cả mặt kỹ thuật mà cả ở quy trình hoạt động kinh doanh của NH nhằm giúp các ngân hàng giữ được sự an toàn cho cả hệ thống an ninh mạng và dữ liệu của họ.

Cuối cùng, công việc trọng tâm là cần phải có kế hoạch hành động khi có xảy ra một cuộc tấn công mạng (nguyên tắc 5). Nếu bị tấn công mạng thì ngân hàng phải nhanh chóng hành động để giữ được lòng tin của khách hàng và giảm thiểu được thiệt hại. Các hành động này bao gồm (i) sửa chữa lỗ hổng bảo mật, (ii) cập nhật kế hoạch bảo mật, (iii) ban hành tuyên bố công khai để củng cố niềm tin của khách hàng. Ngược lại, phản hồi chậm có thể gây bất lợi cho hoạt động của ngân hàng bởi vì sự phản ứng chậm chạp trong những tình huống này có thể gây ra sự thay đổi trong nhận thức của khách hàng và thậm chí nếu không được xử lý tốt thì khách hàng có thể sẽ rời bỏ ngân hàng. Do đó việc thiết kế các kế hoạch hành động nhằm ứng phó với tấn công mạng sẽ là giải pháp then chốt nhằm đảm bảo được sự an toàn và ổn định trong hoạt động kinh doanh ngân hàng.



Hình 4: Lược đồ phản ánh sự phối hợp trong các nhiệm vụ trọng tâm nhằm hạn chế và phòng ngừa rủi ro an ninh mạng của NHTM

Nguồn: Kay và cộng sự (2021)

Hình 4 minh họa các nhiệm vụ trọng tâm và sự kết nối của các nhiệm vụ này khi lập kế hoạch an ninh mạng. Mỗi nhiệm vụ đều quan trọng như nhau và vì thế điều quan trọng là phải phối hợp sao cho đảm bảo sự an toàn trong an ninh mạng cho ngân hàng. Cụ thể, kế hoạch ứng phó sẽ được thực hiện sau khi ngân hàng bị tấn công mạng và các bài học kinh nghiệm từ đó cũng sẽ được sử dụng để cải thiện các kế hoạch hành động, quy trình kỹ thuật và kinh doanh của ngân hàng. Các giải pháp kỹ thuật cần được xem xét để sửa chữa bất kỳ lỗ hổng an ninh mạng nào. Sau khi bị tấn công mạng, các ngân hàng cũng cần phải rà soát toàn bộ hệ thống an ninh mạng

và cả kế hoạch ứng phó của mình. Kế hoạch ứng phó khi đó cũng phải được sửa đổi để cải thiện và gia tăng hiệu quả của các hành động cần thiết nếu có cuộc tấn công mạng diễn ra. Ngoài ra, các chiến lược bảo mật và các chương trình đào tạo nhân viên cũng cần được xem xét và cập nhật để ngăn chặn các mối đe dọa an toàn an ninh mạng trong tương lai.

Để đảm bảo an toàn an ninh mạng, các ngân hàng cần thực hiện đúng theo các nguyên tắc chi tiết được trình bày ở trên. Thực tế chứng minh rằng không có bất kỳ giải pháp an ninh mạng nào có thể áp dụng chung cho tất cả các ngân hàng do sự khác nhau giữa các ngân hàng về cơ sở hạ tầng công nghệ thông tin, các điều kiện về nguồn lực và cả sự ưu tiên trong từng giai đoạn. Do đó, các ngân hàng cũng cần cân nhắc khi thực hiện theo đề xuất trong Hình 4. Tuy nhiên nếu được thực hiện được một cách toàn diện, chúng tôi tin rằng các nguyên tắc và hướng dẫn này sẽ giúp ngân hàng có chiến lược phòng ngừa rủi ro an ninh mạng một cách hiệu quả.

6.4. Giải pháp hạn chế rủi ro an ninh mạng đối mô hình ngân hàng số toàn diện

Hiện một số ngân hàng trên thế giới đã triển khai mô hình ngân hàng số toàn diện, trong đó toàn bộ sản phẩm dịch vụ của ngân hàng được cung cấp trên không gian mạng mà không cần đến sự hiện diện (mang tính vật lý) của bất kỳ chi nhánh ngân hàng nào. Điển hình như ở Brazil, Ngân hàng nhà nước (NHNN) đã cho phép thành lập Ngân hàng số C6 theo mô hình ngân hàng số toàn diện vào ngày 5/8/2019 (Keri Pearlson và cộng sự, 2020). Đây được xem là mô hình ngân hàng số hiện đại nhất có thể giúp tối đa hoá được lợi ích cho khách hàng và tối thiểu hoá chi phí trong cung cấp sản phẩm dịch vụ ngân hàng. Mặc dù chưa có bất kỳ ngân hàng số toàn diện nào được phép thành lập tại Việt Nam nhưng việc thành lập một ngân hàng số toàn diện là hướng đi tất yếu trong quá trình chuyển đổi số ngành ngân hàng hiện nay. Do đó kinh nghiệm trong phát triển mô hình ngân hàng số toàn diện của Brazil sẽ là bài học kinh nghiệm cho các ngân hàng Việt Nam trong thời gian tới.

Về bản chất, Ngân hàng số C6 có rất nhiều khác biệt so với ngân hàng truyền thống. Ví dụ, ngân hàng số C6 sử dụng công nghệ tự động trong kiểm tra chéo thông tin khách hàng với các cơ sở dữ liệu khác nhằm tránh gian lận. Khách hàng của Ngân hàng số C6 sẽ có thể cá nhân hoá giao dịch với ngân hàng. Khách hàng có thể tự thiết kế thẻ tín dụng hoặc thiết lập trang điều hành của ứng dụng theo cách riêng của mình. Chuyển tiền giữa

các tài khoản hoặc thanh toán từ một tài khoản thì rất đơn giản và nhanh chóng. Khi cần hỗ trợ, khách hàng có thể liên hệ với Trung tâm dịch vụ khách hàng vào bất kỳ lúc nào, 7 ngày một tuần, 24 giờ một ngày. Tính đến thời điểm 5/2020, Ngân hàng số C6 đã có 5,570 tài khoản khách hàng. Số lượng nhân viên cũng tăng lên, từ chỉ 25 người sáng lập vào cuối năm 2018 lên 600 nhân viên vào ngày ra mắt, chủ yếu là trong bộ phận phụ trách công nghệ và phát triển sản phẩm.

Do cung cấp sản phẩm hoàn toàn trên không gian mạng, an ninh mạng luôn là sự ưu tiên hàng đầu trong hoạt động của Ngân hàng số C6. Về tổ chức, sự an toàn an ninh mạng tại ngân hàng số C6 được quản lý bởi năm nhóm chính, bao gồm:

(1) Nhóm phòng thủ an ninh mạng: thực hiện giám sát, điều tra và xử lý tất cả các cuộc tấn công mạng và cả các mối đe dọa đến sự an toàn hệ thống mạng của ngân hàng.

(2) Nhóm kỹ thuật an ninh mạng: bao gồm các kỹ sư bảo mật chuyên hỗ trợ nhóm phát triển sản phẩm ngân hàng số. Nhóm cũng chịu trách nhiệm thiết lập tiêu chuẩn thực hành an toàn thông tin và bảo mật điện toán đám mây.

(3) Nhóm quản trị mạng: tập trung vào quản lý rủi ro trong vận hành và đảm bảo tính tuân thủ về tiêu chuẩn an toàn an ninh mạng của toàn bộ ngân hàng. Nhóm cũng quản lý quyền kiểm soát truy cập và nhận dạng người dùng khi họ thực hiện giao dịch với ngân hàng.

(4) Nhóm an toàn ứng dụng: thực hiện kiểm soát, kiểm tra và đưa ra các giải pháp để hỗ trợ và ứng phó kịp thời với các mối đe dọa từ tội phạm mạng tiềm năng. Nhóm cũng điều hành đội an ninh thông tin nhằm chịu trách nhiệm kiểm tra các ứng dụng và cơ sở hạ tầng của Ngân hàng số C6, bao gồm cả kiểm tra sự thâm nhập vào hệ thống lõi của ngân hàng.

(5) Nhóm phụ trách văn hóa an ninh mạng: tập trung vào xây dựng và truyền bá văn hóa an toàn thông tin. Do hoàn toàn khác với mô hình ngân hàng truyền thống, Ngân hàng số C6 phải xây dựng văn hóa công ty cùng với văn hóa an ninh mạng ngay từ thời điểm ngân hàng thành lập. Nhận thức này phải ở trong suy nghĩ của tất cả nhân viên ngân hàng.

Về chiến lược, Ngân hàng số C6 thực hiện đồng thời chiến lược bảo mật theo nguyên tắc *"không tin tưởng bất kỳ ai" (zero-trust)* và các tiêu chuẩn bảo mật cũng như các tiêu chuẩn quốc tế về quản lý ATTT như ISO16 và NIST17. Ngoài ra, rủi ro an ninh mạng luôn được kiểm soát chặt chẽ bằng cách sử dụng mô hình kiểm soát rủi ro 3 lớp. Cụ thể:

(1) Lớp kiểm soát đầu tiên: liên quan đến quy trình hoạt động/ công nghệ/ an toàn thông tin: tất cả các biện pháp phòng thủ được xây dựng ở tất cả các khâu từ chính sách lương thưởng cho đến các lỗ hổng bảo mật, cài đặt phần mềm chống virus, quản lý danh tính và xây dựng tường lửa. Tất cả phần mềm cài đặt luôn được cập nhật và tất cả lỗ hổng an ninh mạng luôn được xử lý bằng các phiên bản mới nhất.

(2) Lớp kiểm soát thứ hai: liên quan đến kiểm soát rủi ro và đảm bảo tính tuân thủ các nguyên tắc bảo mật của ngân hàng. Theo đó, mọi quy trình hoạt động đều được kiểm soát chặt chẽ và được kiểm tra thường xuyên để đảm bảo mọi thứ đều tuân thủ các chính sách an toàn mạng. Hơn nữa, mọi rủi ro đã được xác định cần phải có một kế hoạch để giảm thiểu, loại bỏ hoặc giảm thiểu nó.

(3) Lớp kiểm soát thứ ba: liên quan đến kiểm soát nội bộ: Các kiểm soát viên nội bộ được sử dụng để đảm bảo môi trường kinh doanh số của ngân hàng được bảo mật thông qua các quy trình xác thực và bảo đảm các lỗ hổng bảo mật nằm trong tầm kiểm soát.

Cuối cùng là tập trung vào xây dựng văn hoá an ninh mạng tại ngân hàng. Ngân hàng sử dụng kết hợp các phương thức khác nhau. Ví dụ, các chương trình huấn luyện về an ninh mạng được tổ chức thường xuyên nhằm đảm bảo mỗi cá nhân là một phần của đội ngũ bảo vệ an toàn an ninh mạng của ngân hàng. Các thông tin về rủi ro an ninh mạng, các vụ tấn công mạng luôn được cập nhật thông qua các phương tiện truyền thông nội bộ của ngân hàng. Khuyến khích sự phối hợp giữa các bộ phận chức năng trong phòng và chống rủi ro an ninh mạng tại ngân hàng.

7. KẾT LUẬN

Rủi ro an ninh mạng là một trong những thách thức lớn nhất trong việc chuyển đổi và phát triển ngân hàng số. Bên cạnh việc cung cấp một bức tranh tổng thể về rủi ro an ninh mạng, xu hướng chuyển đổi và phát triển ngân hàng số ở Việt Nam, bài viết tập trung vào phân tích ảnh hưởng

của rủi ro an ninh mạng đến hoạt động ngân hàng số và một số thách thức trong quản trị rủi ro an ninh mạng hiện nay ở Việt Nam.

Để giảm thiểu rủi ro an ninh mạng, các ngân hàng cần thực hiện đồng bộ ba nhóm giải pháp tập trung vào Con người, Công nghệ và Quy trình quản trị rủi ro an ninh mạng. Đối với nhóm giải pháp về Con người, ngân hàng cần (1) thiết kế chương trình đào tạo an ninh mạng cho nhân viên, (2) thực hiện đào tạo an ninh mạng cho khách hàng, và (3) xây dựng các biện pháp an ninh mạng với các đối tác ngân hàng. Với nhóm giải pháp về công nghệ, mỗi ngân hàng nên lựa chọn và tập trung nguồn lực đầu tư vào các công nghệ mang lại giá trị cao, phù hợp với mục tiêu và nguồn lực tài chính của ngân hàng. Hai công nghệ "Trí tuệ nhân tạo (AI)" và công nghệ "Tự động hóa, phản hồi, điều phối và bảo mật (SOAR)" đang được các ngân hàng trên thế giới đánh giá cao nhất trong chiến lược đầu tư công nghệ nhằm giảm rủi ro an ninh mạng. Bên cạnh đó, các ngân hàng cần thiết lập quy trình quản trị rủi ro an ninh mạng hiệu quả, đồng thời phải giám sát hiệu quả việc tuân thủ chặt chẽ quy trình này. Trong bài viết này, chúng tôi đã đề xuất quy trình quản trị rủi ro an ninh mạng tuân theo 5 bước sau: (1) Xác định rủi ro, (2) Phân tích mức độ nghiêm trọng của rủi ro, (3) Đánh giá rủi ro, (4) Ưu tiên các rủi ro và (5) Quyết định cách ứng phó với từng rủi ro.

Để cụ thể hoá các giải pháp giảm thiểu rủi ro an ninh mạng, chúng tôi cũng đề xuất chi tiết các nguyên tắc và hướng dẫn thực hiện. Các hướng dẫn này sẽ được xem như là kim chỉ nam nhằm giúp các ngân hàng nhận định và đánh giá các mối đe dọa an ninh mạng; qua đó có kế hoạch ngăn chặn các vi phạm an ninh mạng và có phương án sẵn sàng ứng phó khi xảy ra các sự cố an ninh mạng. Lưu ý là các phương án này không chỉ đề cập đến yếu tố kỹ thuật của hệ thống CNTT, an ninh mạng của ngân hàng mà còn đề xuất các hướng dẫn chi tiết nhằm ngăn chặn và giảm thiểu đe doạ an ninh mạng trong tương lai.

Cuối cùng, chúng tôi cũng đề xuất thực hiện đồng bộ một số kiến nghị với Chính phủ và Ngân hàng Nhà nước nhằm bảo đảm an ninh mạng cho các ngân hàng ở Việt Nam, đặc biệt trong xu hướng chuyển đổi số.

TÀI LIỆU THAM KHẢO

Tài liệu tiếng Anh

1. Accenture (2020). Cyber threatspace report. https://www.accenture.com/za-en/insights/security/cyber-threatscape-report.
2. Accenture Security (2020). 2020 State of Cyber Resilience: Innovate for Cyber Resilience.
3. Antoine Bouveret (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Papers.

   https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.
4. Apcert (2020). Apcert Annual Report 2020. http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2020.pdf
5. Biener, C., Eling, M., and Wirfs, J. H. (2015). Insurability of Cyber Risk – An Empirical Analysis, The Geneva Papers on Risk and Insurance – *Issues and Practice* 40(1), 131-158.
6. Carmen Ang (2021). The Most Significant Cyber Attacks from 2006-2020, by Country. https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/
7. Cebula, J.J. and Young, L.R. (2010). A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.
8. Cisco (2020). Common cyberattacks. https://www.cisco.com/c/en/us/products/security/commoncyberattacks.html#~how-cyber-attacks-work
9. Cyberreef (2020). Major cyber-attacks 2020. https://www.cyberreef.com/major-cyberattacks-2020/
10. (2017). Blockchain technology: let's discuss. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf
11. Douglas, T., & Loader, B. D. (2000). Cybercrime: Security and surveillance in the information age. Routledge.

12. DTCC (2020). Systemic Risk. https://www.dtcc.com/-/media/Files/Downloads/DTCC-Connection/26362-Systemic-Risk-2020.pdf
13. FBI (2020). Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
14. FinTech News (2020). DDoS Attacks on Financial Institutions: Risks, Consequences, and Prevention. https://www.fintechnews.org/ddos-attacks-on-financial-institutions-risks-consequences-and-prevention/
15. Frank Adelmann và cộng sự (2020). Cyber Risk and Financial Stability: It's a Small World After All. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622.
16. Friedman, S. (2016). Taking cyber risk management to the next level. Deloitte University Press.
17. FSB (2018). Cyber. https://www.fsb.org/2018/11/cyber-lexicon/
18. Goud, N. (2019). List of countries which are most vulnerable to Cyber Attacks, Cybersecurity Insiders.
19. IBM (2020). Cost of data breach report 2020. https://www.ibm.com/security/data-breach
20. IDP (2020). Cybersecurity risks, progress, and the way forward in Latin America and the Caribbean. http://dx.doi.org/10.18235/0002513.
21. Insights (2021). Banking and financial services industry: cyber threat report. https://intsights.com/resources/2021-banking-and-financial-services-industry-cyber-threat-landscape-report
22. Iñaki Aldasoro và cộng sự (2021). Covid-19 and cyber risk in the financial sector. *BIS Bulletin 37*. https://www.bis.org/publ/bisbull37.pdf
23. Johnathan Greg (2019). The 10 most important cyberattacks of the decade. *Tech Republic*. https://www.techrepublic.com/article/the-10-most-important-cyberattacks-of-the-decade/

24. Kay, A. và cộng sự (2021). How financial institutions address cybersecurity threats: A critical analysis. *Issues in Information Systems*, 22(1).

25. Keepersecurity (2020). Nearly 70% of Financial Services Companies Globally Have Experienced a Cyberattack. https://keepersecurity.s3.amazonaws.com/press/pdf/2020/May/FinancialServices.pdf

26. Keri Pearlson và cộng sự (2020). Cybersecurity Culture at C6 Bank. MIT. https://cams.mit.edu/wp-content/uploads/Cybersecurity-Culture-at-C6-Bank-CaseStudy.pdf

27. Kelman, J. (2016). The History of Banking: A Comprehensive Reference Source & Guide. Create Space Independent Publishing Platform.

28. McCrank J. (2013). Nasdaq says software bug caused trading outage. *Reuters.* http://www.reuters.com/article/us-nasdaq-halt-glitch-idUSBRE97S11420130829

29. Microsoft (2018). Advancing Blockchain cybersecurity. Cybersecurity Policy and Resilience, White paper. https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-blockchain-cybersecurity

30. OECD (2020). OECD Digital Economy Outlook 2020. https://www.oecd.org/digital/oecd-digital-economy-outlook-2020-bb167041-en.htm.

31. RAS (2016). Cyber risk appetite: Defining and Understanding Risk in the Modern Enterprise. https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf

32. Steve Morgan (2021). Special Report: Cyberwarfare In The C-Suite. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

33. Skinner, C. (2014). Digital Bank: Strategies to launch or become a digital. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=digital+bank%3A+strategies+to+launch+or+become+a+digital+bank&btnG=

34. SCN Education B.V. (2001). Electronic Banking: The Ultimate Guide to Business and Technology of Online Banking. Springer Science & Business Media.

35. Scardovi, C. (2017). Digital Transformation in Financial Services. Springer

36. Wall, D. (2001). Cybercrimes and the Internet. Crime and the Internet. Routledge.

37. WEF (World Economic Forum) (2020a). The Global Risks Report 2020. https://www.weforum.org/reports/the-global-risks-report-2020.

38. WEF (World Economic Forum) (2020b). COVID-19 Risks Outlook: A Preliminary Mapping and Its Implications. https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications.

Tài liệu tiếng Việt

1. Du Lam (2020). Facebook xóa hàng trăm nghìn bài viết, Google chặn 18 triệu email Covid-19 độc hại mỗi ngày. *Vietnamnet*. https://vietnamnet.vn/vn/cong-nghe/facebook-xoa-hang-tram-nghin-bai-viet-google-chan-18-trieu-email-covid-19-doc-hai-moi-ngay-634436.html

2. Hà An (2020). Lỗ hổng trong an ninh thông tin ngân hàng số. *Nhân dân điện tử*. https://nhandan.com.vn/chuyen-de-cuoi-tuan/lo-hong-trong-an-ninh-thong-tin-ngan-hang-so-616515/

3. Hồng Vinh (2021), Tội phạm mạng: Ngân hàng vẫn là đích ngắm. *Thời báo kinh tế Việt Nam*. https://vneconomy.vn/toi-pham-mang-ngan-hang-van-la-dich-ngam.htm.

4. Huyền Anh (2020). Thiệt hại 100 tỷ đồng từ 4.000 vụ tấn công an ninh mạng của ngân hàng. *Thời báo kinh doanh*. https://vnbusiness.vn/ngan-hang/thiet-hai-100-ty-dong-tu-4-000-vu-tan-cong-an-ninh-mang-cua-ngan-hang-1075009.html

5. Lâm Thảo (2021). Toàn cảnh an ninh mạng Việt Nam năm 2020: Tổn thất hơn 1 tỷ USD do virus máy tính. *Nhân dân điện tử*. https://nhandan.com.vn/thong-tin-so/toan-canh-an-ninh-mang-viet-nam-nam-2020-ton-that-hon-1-ty-usd-do-virus-may-tinh-632235/

6. Ngọc Khang (2021). VPBank tổ chức Hội thảo "Phòng ngừa, đấu tranh tội phạm sử dụng công nghệ cao trong lĩnh vực ngân hàng". http://cand.com.vn/Kinh-te/VPBank-to-chuc-Hoi-thao-Phong-ngua-dau-tranh-toi-pham-su-dung-cong-nghe-cao-trong-linh-vuc-ngan-hang-626485/
7. Nguyễn Vũ (2019). Ngân hàng tăng cường bảo mật trước rủi ro an ninh mạng. *Tạp chí tài chính*. https://tapchitaichinh.vn/ngan-hang/ngan-hang-tang-cuong-bao-mat-truoc-rui-ro-an-ninh-mang-308196.html.
8. Phạm Tiến Dũng (2021). Chuyển đổi số - Xu hướng tất yếu trong hoạt động ngân hàng. *Tạp chí ngân hàng*. http://tapchinganhang.gov.vn/chuyen-doi-so-xu-huong-tat-yeu-trong-hoat-dong-ngan-hang.htm.

PHỤ LỤC

Phụ lục 1: Chi tiết 20 biện pháp kiểm soát an ninh mạng được đề xuất bởi CIS (Trung tâm An ninh Internet)

(1) Kiểm kê và kiểm soát tài sản phần cứng: quản lý tích cực tất cả các thiết bị phần cứng được phép có quyền truy cập mạng để ngăn các thiết bị trái phép truy cập.

(2) Kiểm kê và kiểm soát tài sản phần mềm: yêu cầu kiểm kê (theo dõi, phân tích, sửa và xóa) tất cả phần mềm được cài đặt trên mạng. Điều này nhằm đảm bảo rằng phần mềm trái phép không được cài đặt hoặc thực thi.

(3) Quản lý lỗ hổng liên tục: phải liên tục xác định các điểm yếu và lỗ hổng bảo mật và khắc phục hiệu quả chúng.

(4) Sử dụng có kiểm soát các Đặc quyền quản trị: yêu cầu theo dõi và quản lý những người có đặc quyền quản trị. Đây là những người có quyền thực hiện bất kỳ thay đổi nào mà họ mong muốn như cho phép người dùng khác truy cập vào mạng hay cài đặt hoặc thực thi các chương trình.

(5) Cấu hình an toàn cho phần cứng và phần mềm trên thiết bị di động, máy tính xách tay, máy trạm và máy chủ. Quản lý an ninh mạng thông qua các giao thức cấu hình và quản lý thay đổi phần cứng và phần

mềm nghiêm ngặt. CIS chỉ định việc theo dõi, báo cáo và hiệu chỉnh nghiêm ngặt các cấu hình bảo mật cho tất cả phần cứng và phần mềm trên các thiết bị di động, máy trạm và máy chủ.

(6) Bảo trì, giám sát và phân tích nhật ký kiểm tra: yêu cầu các tổ chức phải duy trì một tài khoản chi tiết về tất cả các sự kiện xảy ra trên mạng. Quá trình này có thể giúp ích trong trường hợp vi phạm. Phân tích nhật ký có thể giúp xác định vị trí có thể bắt đầu vi phạm và mức độ hệ thống đã bị xâm phạm.

(7) Bảo vệ trình duyệt web và email: yêu cầu bảo vệ nâng cao cho email và hoạt động của trình duyệt web để giảm thiểu nguy cơ bị kẻ tấn công thao túng nhân sự.

(8) Phòng thủ phần mềm độc hại: kiểm soát và quản lý sự lây lan hoặc thực thi phần mềm độc hại bằng cách sử dụng biện pháp bảo vệ nếu có. Việc sử dụng các quy trình tự quản có thể chủ động quét, loại bỏ các mối đe dọa và sửa chữa hoặc cập nhật biện pháp phòng thủ được khuyến khích.

(9) Giới hạn và kiểm soát các cổng mạng, giao thức và dịch vụ: quản lý tích cực việc sử dụng các cổng, giao thức và dịch vụ, thực hiện các chỉnh sửa cần thiết để giảm thiểu các lỗ hổng.

(10) Khả năng khôi phục dữ liệu: phải có một quy trình và phương pháp luận đã được chứng minh để sao lưu và phục hồi kịp thời thông tin quan trọng.

(11) Cấu hình an toàn cho các thiết bị mạng, chẳng hạn như tường lửa, bộ định tuyến và thiết bị chuyển mạch: bảo vệ các thiết bị cơ sở hạ tầng mạng thông qua việc quản lý tích cực cấu hình bảo mật của chúng thông qua việc theo dõi và báo cáo các lỗ hổng và sửa chữa hiệu quả của chúng.

(12) Phòng thủ ranh giới: yêu cầu sửa chữa, phát hiện và ngăn chặn thông tin nhạy cảm được chuyển giữa các mạng có mức độ tin cậy khác nhau.

(13) Bảo vệ dữ liệu: đòi hỏi các quy trình và công cụ được thiết kế đặc biệt để bảo vệ. Dữ liệu phải được phân loại theo mức độ nhạy cảm và các mức độ bảo vệ liên quan được áp dụng tương ứng, bao gồm cả mã hóa để giảm thiểu rủi ro khi dữ liệu đã bị tách ra.

(14) Quyền truy cập có kiểm soát dựa trên nhu cầu cần biết: yêu cầu hạn chế quyền truy cập vào các tài sản và thông tin quan trọng đối với cá nhân.

(15) Kiểm soát truy cập không dây: Mạng cục bộ không dây (WLAN), hệ thống không dây dành cho khách hàng và điểm truy cập không dây phải được quản lý tích cực thông qua các quy trình và thủ tục theo dõi, kiểm soát, phát hiện và ngăn chặn hoạt động độc hại. Kênh và nhân viên dựa trên mức độ tin cậy của các cá nhân bên trong tổ chức (phân loại đã được phê duyệt). Điều này có nghĩa là chỉ những người trong tổ chức cần quyền truy cập vào thông tin hoặc nội dung đó mới có quyền truy cập.

(16) Giám sát và kiểm soát tài khoản: xóa hoặc ngừng hoạt động của các tài khoản không hoạt động và việc tạo tài khoản mới được giám sát chặt chẽ.

(17) Triển khai Chương trình đào tạo và nhận thức về an ninh: tăng cường nhận thức của nhân sự về các vấn đề bảo mật và đào tạo về các lỗ hổng bảo mật.

(18) Bảo mật phần mềm ứng dụng: phải tích cực quản lý các tiêu chuẩn bảo mật của phần mềm. Điều này giúp tổ chức có thể sửa chữa, ngăn chặn và theo dõi các điểm yếu về bảo mật.

(19) Ứng phó và quản lý sự cố: phát triển và triển khai cơ sở hạ tầng ứng phó sự cố hiệu quả bao gồm tất cả các yếu tố cần thiết để phát hiện, ứng phó, giảm thiểu và loại bỏ các cuộc tấn công một cách nhanh chóng và hiệu quả.

(20) Thử nghiệm thâm nhập và bài tập cho đội đỏ: thử nghiệm thực tế tất cả các biện pháp kiểm soát trên. Với thử nghiệm thâm nhập, tổ chức có thể mô phỏng một cuộc tấn công trên mạng. Bằng cách này, họ có thể xem liệu vẫn còn lỗ hổng có thể bị khai thác hay không.

Phụ lục 2: Đặc điểm công nghệ Blockchain trong đảm bảo an toàn an ninh mạng

Công nghệ Blockchain đang trở thành một trong những công nghệ được sử dụng phổ biến trong kinh tế toàn cầu. Không chỉ giới hạn ở các ứng dụng kinh tế, công nghệ này cũng được sử dụng trong quản lý an toàn an ninh mạng. Theo Microsoft (2018), có rất nhiều ưu điểm khi sử dụng công nghệ Blockchain, bao gồm:

- Sự phân tán trong lưu trữ dữ liệu: các cuộc tấn công mạng thường nhắm vào các cơ sở dữ liệu tập trung; qua đó làm lây nhiễm và mất ổn định của cả hệ thống. Tuy nhiên, với đặc tính dữ liệu được phân tán, công nghệ Blockchain sẽ giúp hệ thống CNTT của tổ chức phục hồi hoạt động tốt hơn khi bị tấn công mạng. Bởi vì các cuộc tấn công mạng sẽ không làm mất dữ liệu hoặc xâm phạm đến dữ liệu đã được lưu trên các "khối" trước đó.
- Cơ chế xác nhận đồng thuận: đây là cơ chế mà công nghệ Blockchain sẽ yêu cầu phải có sự đồng nhất của một số lượng nút (nodes) nhất định nếu muốn chia sẻ một khối dữ liệu mới trong chuỗi. Ngoài ra cơ chế xác nhận này cũng sẽ được thực hiện liên tục nhằm kiểm tra tính toàn vẹn của các giao dịch trong quá khứ đã được ghi nhận trước đó và giúp phát hiện các giao dịch mới không an toàn cho hệ thống.
- Mã hóa: đây là cơ chế cho phép tích hợp nhiều hình thức mã hóa khác nhau tại các điểm khác nhau. Do đó, công nghệ Blockhain sẽ giúp cung cấp nhiều lớp bảo vệ cho người dùng. Cụ thể, quyền truy cập sẽ được bảo mật thông qua các biện pháp mã hóa mật mã người dùng. Các liên kết, khối liên kết cũng sẽ được mã hóa, và bảo mật bằng chữ ký số hoặc mã hóa.
- Tính minh bạch: tính minh bạch của chuỗi khối sẽ gây nhiều khó khăn hơn cho các cuộc tấn công mạng cũng như lấy cắp dữ liệu bởi mỗi người tham gia đều có quyền kiểm soát dữ liệu như nhau.

Tuy nhiên, công nghệ Blockchain cũng tồn tại các rủi ro nếu công nghệ này được đưa vào sử dụng trong quản lý an ninh mạng. Một số những rủi ro có thể kể đến:

- Quản lý khóa (mã số): đây là rủi ro chính yếu nhất củng công nghệ Blockchain. Nếu cá nhân làm mất mã số thì sẽ không thể khôi phục và vì thế dẫn đến mất dữ liệu, tài sản trên công nghệ blockchain.
- Lỗi mã hóa phần mềm/ lỗ hổng giao thức: tương tự như bất kỳ hệ thống CNTT nào, lỗi mã hóa của con người có thể dẫn đến nguy cơ đe doạ an toàn an ninh mạng. Công nghệ Blockchain được xây dựng dựa trên các mã phần mềm, và trên thực tế không có bất cứ phần mềm nào là không có lỗi và đều có khả năng bị xâm phạm bởi các tội phạm mạng.

- Nguồn dữ liệu ngoài và rủi ro điểm cuối (endpoint): công nghệ Blockchain sẽ chỉ an toàn khi sử dụng những thông tin được nhập vào hệ thống và được sử dụng sau đó. Tuy nhiên, công nghệ Blockchain vẫn kết nối và hoạt động dựa vào các nguồn dữ liệu bên ngoài. Hệ thống kế thừa (legacy systems) của người tham gia vào các ứng dụng Blockchain là một nguồn dữ liệu bên ngoài. Việc nhập dữ liệu từ các hệ thống ngoài chuỗi (off-chain), vì thế, sẽ tạo ra dữ liệu được lưu lại trên các khối, từ đó dẫn đến rủi ro điểm cuối.
- Tấn công dựa trên danh tính: giống như các hệ thống CNTT khác, các blockchain vẫn có nguy cơ là mục tiêu của những cuộc tấn công mạng dưới hình thức giả mạo danh tính. Các cuộc tấn công này có thể chiếm phần lớn các nút (nodes) trong mạng lưới và phá hoại kiến trúc phân tán, vốn là đặc trưng nổi trội của công nghệ Blockchain.
- Các rủi ro mới: ví dụ các cuộc tấn công dựa trên tính toán lượng tử, tận dụng việc tính toán nâng cao để làm suy yếu hoặc làm tổn hại các thuật toán mật mã hiện được sử dụng trong các hệ thống CNTT có sử dụng công nghệ Blockchain.