# Khảo sát về Niềm tin số toàn cầu 2022

## Góc nhìn Việt Nam

**Nghiên cứu của PwC**

Tháng 2/2022

pwc

# Mục lục

# Khảo sát về niềm tin số năm 2022

## Phạm vi toàn cầu

**3,602**
quản lý cao cấp kinh doanh, công nghệ và bảo mật, bao gồm 633 người đến từ Châu Á - Thái Bình Dương (Châu Á - TBD)

**33%**
nữ

**20+**
năm liên tiếp

**62%**
công ty vốn hóa trên 1 tỷ đô la Mỹ

**33%**
công ty vốn hóa trên 10 tỷ đô la Mỹ

# Bối cảnh bảo mật toàn cầu có dấu hiệu tiêu cực

69% các tổ chức trên thế giới dự đoán sẽ gia tăng mức chi tiêu vào không gian mạng trong năm 2022, so với số liệu khảo sát 55% của năm trước. Điều này được thể hiện rõ ràng hơn ở khu vực Châu Á - TBD - 77% các tổ chức dự báo sẽ gia tăng ngân sách không gian mạng tại doanh nghiệp họ.

Doanh nghiệp tiếp tục đầu tư vào an ninh mạng vì họ nhận thức được các rủi ro đang ngày một gia tăng. Trong Khảo sát về niềm tin số toàn cầu năm 2022, hơn 50% đáp viên trên toàn cầu và khu vực Châu Á - TBD dự đoán số lượng các sự cố mạng sẽ tăng mạnh so với năm 2021. Phát hiện này cũng nhất quán với kết quả của Khảo sát CEO toàn thường niên lần thứ 25, trong đó rủi ro an ninh mạng được cho là rủi ro hàng đầu đối với triển vọng doanh nghiệp bởi các CEO toàn cầu và là rủi ro thứ hai đối với các CEO khu vực Châu Á - TBD - chỉ sau rủi ro y tế, sức khỏe.

Năm 2021 là một trong những thời điểm ghi nhận nhiều rủi ro về an ninh mạng nhất. Theo báo cáo về Triển vọng An ninh mạng Toàn cầu 2022, số lượng các cuộc tấn công thông qua mã độc tống tiền đã tăng 151% chỉ trong nửa đầu năm 2021. Tương tự tại Việt Nam, Trung tâm Giám sát an toàn không gian mạng Quốc gia Việt Nam (NCSC) đã ghi nhận 1.383 cuộc tấn công mạng trong tháng đầu năm 2022, tăng mạnh 10,29% so với tháng 12/2021.

Có thể thấy những kẻ tấn công tinh vi đang nhân mọi cơ hội khai thác các lỗ hổng chống lại con người, tổ chức cũng như cơ sở hạ tầng quan trọng thông qua công nghệ. Và xu hướng này được dự đoán sẽ tiếp tục gia tăng trong thời gian tới.

Hậu quả của những cuộc tấn công mạng trở nên nặng nề hơn khi các hệ thống ngày càng phụ thuộc vào nhau một cách phức tạp hơn. Các cơ sở hạ tầng quan trọng đặc biệt dễ bị tổn thương. Tuy nhiên, những rủi ro này vẫn có thể ngăn ngừa được bằng các thông lệ tốt và kiểm soát chặt chẽ.

Để đáp ứng nhu cầu của thị trường Việt Nam, báo cáo này được trích từ Khảo sát về niềm tin số toàn cầu năm 2022 của PwC, được công bố vào tháng 11/2021. Báo cáo cung cấp các hướng dẫn nhằm đơn giản hóa chiến lược bảo mật, đồng thời giải quyết những lo ngại xoay quanh vấn đề liệu các tổ chức đã trở nên quá phức tạp để bảo mật khỏi những rủi ro an ninh mạng và quyền riêng tư vốn dĩ có thể tránh được.

# An ninh mạng tiếp tục là ưu tiên hàng đầu của Việt Nam

Nền kinh tế số của Việt Nam được dự báo sẽ vượt mức 43 tỷ đô la Mỹ vào năm 2025 khi đất nước tiếp tục phát triển các dự án về chính phủ điện tử, vạn vật kết nối, thành phố thông minh, công nghệ tài chính, trí tuệ nhân tạo, v.v.. Không gian mạng đang xóa nhòa ranh giới khu vực và quốc gia. Việt Nam sẽ phải đối mặt với các hiểm họa mạng ngày một gia tăng và các cuộc tấn công tinh vi hơn.

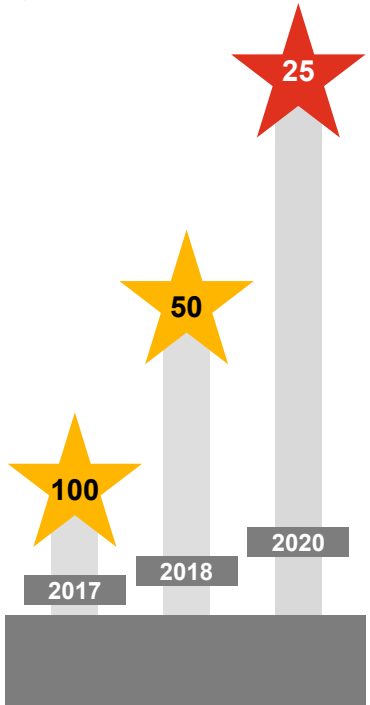
Trong những năm gần đây, Chính phủ Việt Nam đã ban hành nhiều quy định nhằm phát triển thị trường an ninh mạng nội địa, bao gồm:

- Chỉ thi số 22 / CT-BTTTT được ban hành vào tháng 5/2021 của Bộ Thông tin và Truyền thông tập trung tăng cường công tác phòng, chống vi phạm pháp luật và tội phạm trên Internet.
- Quyết đinh 1907 / QĐ-TTg được ban hành năm 2020 phê duyệt bởi Bộ Thông tin và Truyền thông nhằm nâng cao nhận thức và phổ biến kiến thức về an toàn thông tin cho giai đoạn 2021-2025.
- Chỉ thi số 14 / CT-TTg của Thủ tướng Chính phủ được ban hành vào tháng 6/2019 đã tăng cường các biện pháp an toàn về an ninh mạng cho khu vực công, trong đó, ngân sách cho an ninh mạng phải chiếm ít nhất 10% tổng chi tiêu Công nghệ thông tin hàng năm của doanh nghiệp trong giai đoạn 2020-2025.
- Dự thảo Nghi đinh về Bảo vệ Dữ liệu Cá nhân, một khi được ban hành, nghị định này được kỳ vọng trở thành bộ luật toàn diện đầu tiên về dữ liệu cá nhân.

Những nỗ lực này đã mang lại những kết quả tích cực. Năm 2020, Việt Nam được xếp hạng thứ 25 trên tổng 194 quốc gia về Chỉ số An ninh mạng Toàn cầu (GCI). Đây là một sự cải thiện đáng kể so với năm 2018 và 2017 khi Việt Nam lần lượt được xếp ở vị trí 50 và 100. Kết quả này còn vượt mục tiêu của Việt Nam là lọt vào top 30 quốc gia hàng đầu của GCI vào năm 2030 theo Quyết định số 749 / QĐ-TTg ngày 3/6/2020 của Thủ tướng Chính phủ.

Xếp hạng GCI của Việt Nam

Nguồn: Liên minh Viễn thông Quốc tế GCI



# Đơn giản hóa an ninh mạng có chủ đích

Khảo sát về niềm tin số toàn cầu năm 2022 hướng dẫn các tổ chức phương pháp tối ưu hóa các hoạt động và quy trình một cách có chủ đích và cẩn trọng. Báo cáo tập trung vào bốn câu hỏi lớn, bắt đầu từ phía CEO, nhằm thiết lập một cách tiếp cận thống nhất đối với an ninh mạng. Những câu hỏi này thường bị bỏ qua, tuy nhiên, nếu được cân nhắc kỹ lưỡng, những câu hỏi này có thể mang lại kết quả đáng kể.

1. CEO làm thế nào để tạo ra sự khác biệt trong doanh nghiệp họ?
2. Liệu doanh nghiệp đã trở nên quá phức tạp để bảo mật?
3. Làm cách nào để biết liệu doanh nghiệp mình có đang được bảo vệ trước những rủi ro quan trọng nhất hay không?
4. Liệu doanh nghiệp đã hiểu rõ những rủi ro liên qua đến bên thứ ba và chuỗi cung ứng?

Phần tiếp theo của báo cáo sẽ diễn giải chi tiết các phát hiện của chúng tôi.

Top 10% đáp viên báo cáo những bước tiến đáng kể hướng tới các mục tiêu an ninh mạng quan trọng[1] - có thể gọi là nhóm có nhiều cải thiện nhất - có khả năng thực hiện các chiến lược đúng đắn, gấp nhiều lần so với các đáp viên khác. Dưới đây minh họa hiệu ứng cấp số nhân của phương pháp đơn giản hóa an ninh mạng.

**12 lần** Họ nói rằng CEO hỗ trợ họ khi cần - nhiều hơn gấp 12 lần.

**5 lần** Họ có những hoạt động hợp lý toàn doanh nghiệp - nhiều hơn gấp 5 lần.

**10 lần** Họ có một quy trình chính thức được thực hiện đầy đủ cho bảo mật thông tin - nhiều hơn gấp 10 lần.

**11 lần** Họ có hiểu biết tốt về rủi ro không gian mạng và quyền riêng tư từ các bên thứ ba - nhiều hơn gấp 11 lần.

[1] Mục tiêu an ninh mạng bao gồm việc thấm nhuần văn hóa an toàn bảo mật, quản lý rủi ro mạng, tăng cường giao tiếp giữa các hội đồng và ban quản lý, và điều phối chiến lược bảo mật cùng chiến lược kinh doanh.


CEO làm thế nào để tạo ra
sự khác biệt trong doanh nghiệp họ?

# Các CEO tham gia vào hoạt động an ninh mạng như thế nào?

Khảo sát của chúng tôi cho thấy sự chênh lệch rõ rệt về kỳ vọng liên quan đến an ninh mạng:

- Các đáp viên cho rằng các CEO tham gia vào các hoạt động an ninh mạng khi khủng hoảng xảy ra. Các CEO nhận thấy bản thân họ đang tham gia nhiều hơn.
- Các CEO tin rằng họ hỗ trợ 'đáng kể' về các vấn đề xoay quanh an ninh mạng, nhưng chỉ 3/10 các đáp viên không phải CEO đồng ý với điều này.

Đã đến lúc thu hẹp khoảng cách giữa các CEO và các quản lý cấp cao C-suite khác về mức độ tham gia của CEO và hỗ trợ của họ cho an ninh mạng. Nếu không, khoảng cách này có thể gây ra thảm họa khi mang lại cảm giác an toàn sai lầm trên toàn doanh nghiệp, vì CEO có vai trò tối quan trọng trong việc định hướng văn hóa tổ chức.

**Các CEO có quyền lực và tiềm năng phát triển chiến lược đến an ninh mạng.** Trong "nhóm các công ty có nhiều cải thiện nhất" (những công ty có chiến lược bảo mật tốt nhất trong hai năm qua), các CEO đã hỗ trợ trên mọi lĩnh vực nhiều hơn gấp **14 lần**. Khảo sát tiếp tục chỉ ra các quản lý cấp cao ở hầu hết các khu vực và ngành công nghiệp cho rằng phương pháp tối quan trọng để hướng tới một xã hội số an toàn vào năm 2030 là giáo dục các CEO và hội đồng quản trị để họ có thể hoàn thành tốt hơn các nhiệm vụ và trách nhiệm an ninh mạng của mình.

**Các đáp viên cho rằng các CEO tham gia vào các hoạt động an ninh mạng khi khủng hoảng mạng xảy ra. CEO nghĩ rằng họ đang tham gia nhiều hơn**

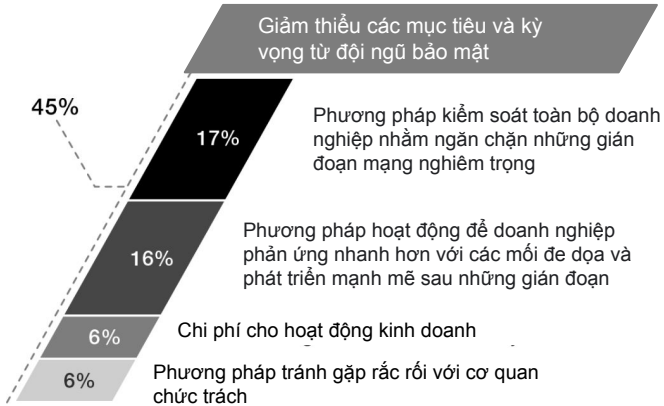

Câu hỏi: Vấn đề bảo mật và quyền riêng tư nào sau đây, bạn / CEO của bạn sẽ trực tiếp tham gia? Hãy sắp xếp chúng theo thứ tự.
Cơ sở: đáp viên không phải CEO: 2,929, đáp viên CEO:673
Nguồn: PwC, Khảo sát niềm tin số toàn cầu, tháng 10 năm 2021

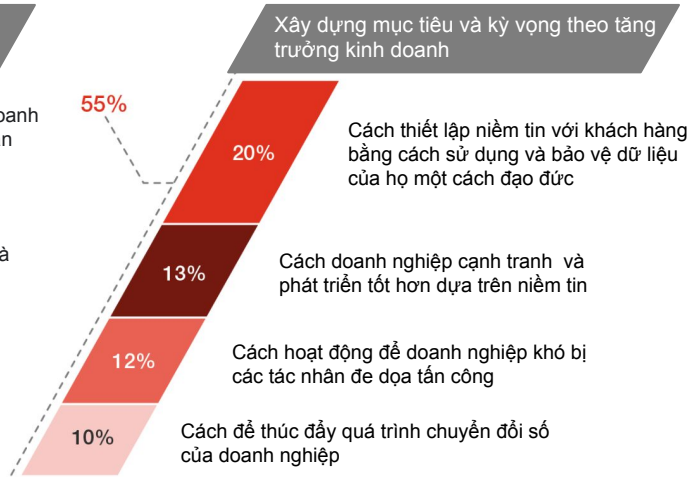
# Thay đổi mục tiêu bảo mật:
# Xây dựng niềm tin và tăng trưởng kinh doanh

Mục tiêu bảo mật đang dần chuyển đổi sang xây dựng niềm tin và tăng trưởng kinh doanh, với 54% đặt mục tiêu trên khả năng phòng thủ và kiểm soát bảo mật.

| Mục tiêu | Thế giới | Châu Á - TBD |
|---|---|---|
| Tăng khả năng ngăn chặn các cuộc tấn công | Hạng 1 | Hạng 2 |
| Gia tốc thời gian phản hồi đối với các sự cố và gián đoạn | Hạng 2 | Hạng 3 |
| Cải thiện niềm tin của các lãnh đạo vào khả năng quản lý các mối đe dọa hiện tại và tương lai của tổ chức | Hạng 3 | Hạng 1 |

Ở cả nhóm CEO và nhóm không phải CEO, “xây dựng niềm tin với khách hàng thông qua sử dụng dữ liệu một cách có đạo đức và bảo vệ dữ liệu của họ" là lựa chọn hàng đầu cho mục tiêu bảo mật. Tất cả đều đồng ý với việc phòng ngừa là cơ sở quan trọng nhất; tiếp theo là khả năng phục hồi; và xây dựng niềm tin (bao gồm niềm tin của người tiêu dùng: “cải thiện trải nghiệm khách hàng” và “mức độ trung thành của khách hàng cao hơn” được xếp hạng tiếp theo trong danh sách).



# Những điểm đáng lưu ý

Các mục tiêu hàng đầu cho an ninh mạng trong 3 năm là:

- Tăng khả năng ngăn chặn các cuộc tấn công (mục tiêu này xếp thứ ba đối với các công ty trong lĩnh vực năng lượng và tiện ích)
- Gia tốc thời gian phản hồi đối với các sự cố và gián đoạn
- Cải thiện niềm tin của các lãnh đạo vào khả năng quản lý các mối đe dọa hiện tại và tương lai của tổ chức (đứng đầu trong lĩnh vực năng lượng, tiện ích và tài nguyên)

**CEO:**

- Đặt vấn đề an ninh mạng là quan trọng đối với tiềm năng phát triển kinh doanh và xây dựng niềm tin với khách hàng - không chỉ phòng thủ và kiểm soát - nhằm tạo ra một tư duy bảo mật cho toàn doanh nghiệp
- Thể hiện sự tin tưởng và kiên định ủng hộ CISO (giám đốc an ninh thông tin)
- Đối diện với các vấn đề và rủi ro trong mô hình kinh doanh và thay đổi những gì cần thiết. CEO sẽ có rất nhiều cơ hội để làm theo lời khuyên của Peter Drucker: “Quản lý đang làm những điều đúng đắn; lãnh đạo đang làm những điều đúng đắn.”

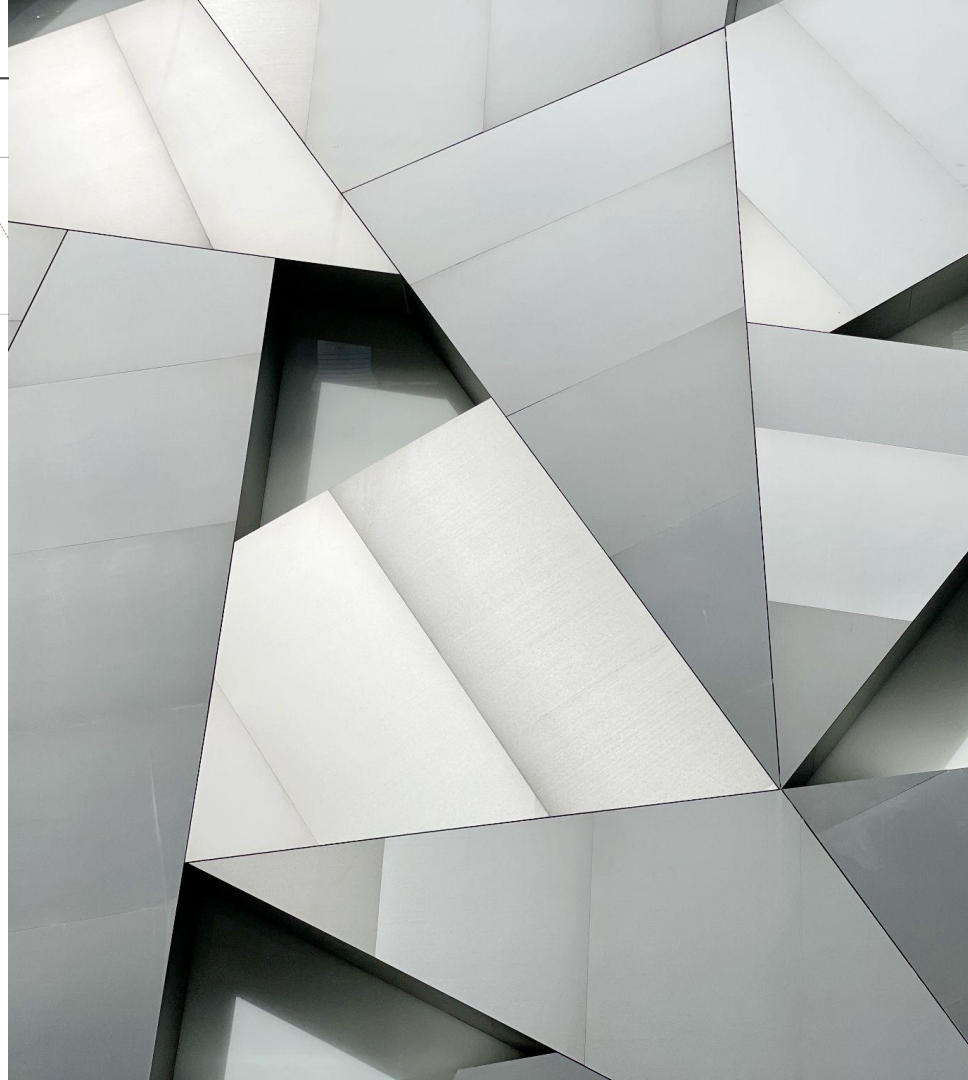
**Giám đốc an ninh thông tin (CISO):**

- Thấu hiểu chiến lược kinh doanh của tổ chức
- Xây dựng mối quan hệ bền chặt hơn với CEO và trao đổi thường xuyên để hỗ trợ CEO trong chiến lược đơn giản hóa an ninh mạng
- Trang bị cho mình những kỹ năng cần để phát triển mạnh mẽ trong môi trường mà vai trò của an toàn bảo mật ngày càng phát triển và mở rộng. Và định hướng lại các nhóm, hướng tới giá trị kinh doanh và niềm tin của khách hàng.

“

An ninh mạng của mỗi tổ chức bắt đầu và kết thúc ở cấp quản lý cao nhất. 70% các CEO được khảo sát đồng ý rằng ngân sách cho an ninh mạng trong năm 2022 sẽ được tăng lên. Trước bối cảnh những rủi ro ngày càng tăng cao, an ninh mạng không chỉ là vấn đề của “kiểm soát nội bộ” mà còn là một công cụ quan trọng hỗ trợ các tổ chức xây dựng lòng tin với khách hàng và tăng trưởng kinh doanh bền vững.

**Bà Nguyễn Phi Lan**
Phó Tổng giám đốc, Lãnh đạo dịch vụ Tư vấn Quản lý Rủi ro, PwC Việt Nam



# Liệu doanh nghiệp

# đã trở nên quá phức tạp để bảo mật?

# Liệu các doanh nghiệp hiện nay có quá phức tạp?

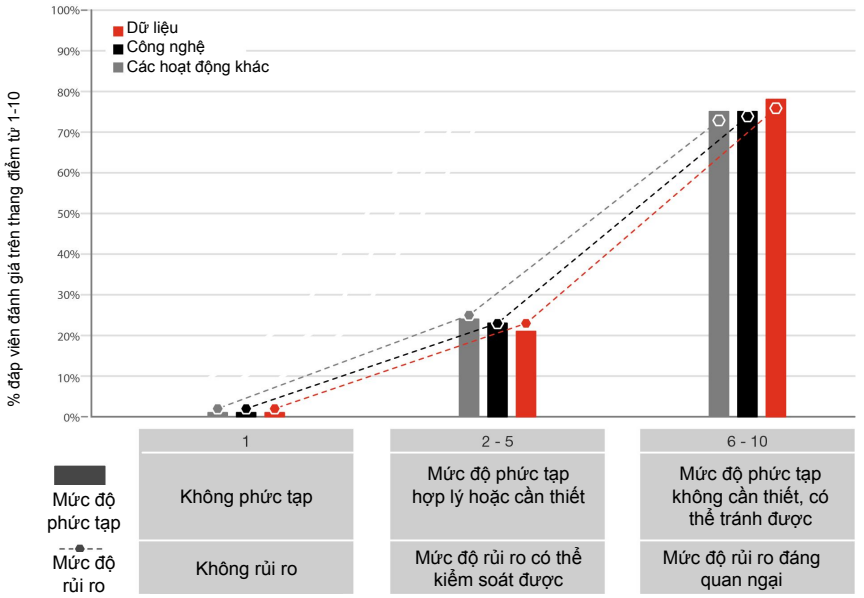
Điểm đáng lo ngại nhất của sự phức tạp này là các CEO đã chấm mức độ phức tạp 10 cho 7 trong số 11 lĩnh vực trong doanh nghiệp của họ. Các phát hiện khác cho thấy:

- 75% các quản lý cao cấp báo cáo có nhiều sự phức tạp có thể tránh được và không cần thiết hiện hữu trong tổ chức, trong công nghệ, dữ liệu và môi trường hoạt động của họ.
- Cũng khoảng 75% tin rằng sự phức tạp dẫn đến rủi ro đáng lo ngại về an ninh mạng và quyền riêng tư.

**Đơn giản hóa cần đầu tư nhiều thời gian và công sức nhưng mang lại hiệu quả cao.**

- Các công ty thuộc nhóm "cải thiện nhiều nhất" có khả năng sắp xếp các hoạt động một cách hợp lý trên toàn doanh nghiệp cao hơn gấp 5 lần. Họ chú trọng vào:
  - hợp nhất các nhà cung cấp công nghệ (62%),
  - xác định / tái thiết lập sự kết hợp giữa dịch vụ nội bộ và dịch vụ được quản lý (60%),
  - tổ chức lại chức năng và cách thức làm việc (59%).
- Đơn giản hóa an ninh mạng, chủ yếu là chuyển đổi đám mây, có thể hỗ trợ hợp lý hóa các quy trình kinh doanh và kiến trúc CNTT, cung cấp tính linh hoạt và tăng tốc quá trình đổi mới.

**75% quản lý cao cấp cho rằng doanh nghiệp của họ quá phức tạp, dẫn đến những rủi ro "đáng quan ngại" về bảo mật và quyền riêng tư**




Câu hỏi: Theo bạn, các hoạt động doanh nghiệp sau đây phức tạp đến mức nào, trên thang điểm từ 1 đến 10? Các lỗ hổng trong bảo mật và quyền riêng tư tạo nên bởi những sự phức tạp trên nghiêm trọng ở mức độ nào?
Cơ sở: 3,602 người trả lời
Nguồn: PwC, Khảo sát niềm tin số toàn cầu, tháng 10 năm 2021

# Những điểm đáng lưu ý

Các hoạt động được hợp lý hóa trong 2 năm qua:

- Hợp nhất các nhà cung cấp công nghệ (62%),
- Xác định/tái thiết lập sự kết hợp giữa các dịch vụ nội bộ và được quản lý (60%),
- Tổ chức lại các chức năng và cách làm việc (59%) và
- Xây dựng khung quản trị dữ liệu tích hợp (58%).

**Các COO và quản lý chuyển đổi**
Câu hỏi: Kế hoạch bảo mật cho điều này là gì? Bạn có thể đốt cháy những thay đổi lớn - trong hoạt động và văn hóa - chỉ đơn giản bằng cách đặt câu hỏi này cho mọi quản lý cao cấp phụ trách một sáng kiến chuyển đổi hoặc kinh doanh mới. Bằng cách đặt an ninh mạng lên trọng tâm hàng đầu, bạn sẽ tránh được những sự phức tạp không cần thiết và tốn kém ngay bây giờ.

Để CISO và các nhóm bảo mật tham gia vào quá trình chuyển đổi và áp dụng điện toán đám mây, mua bán và sáp nhập, và các sáng kiến khác.

**CISO và CIO**: Dám “làm phép trừ”, để công nghệ và dữ liệu tự “nhân”, “chia” và chinh phục tính hiệu quả và bảo mật. Có thể, bạn sẽ vô tình thêm độ phức tạp với số lượng công cụ bảo mật bạn muốn thêm vào. Thay vào đó, hãy giảm bớt sự dư thừa và ghi nhớ các mục tiêu bảo mật như: đánh giá các kho dữ liệu và loại bỏ những dữ liệu không cần thiết; chuyển các ứng dụng và giải pháp vào môi trường đám mây để quản lý dễ dàng hơn; và hợp nhất, thanh lý, chuẩn hóa và tự động hóa khi có thể.

Ngoài ra, hãy xem xét lại quy trình đầu tư công nghệ và an ninh mạng. Đầu tiên, hãy tập trung vào việc đơn giản hóa những điểm mang lại lợi ích lớn nhất cho toàn bộ doanh nghiệp.


Bảo mật chống lại
các rủi ro quan trọng
đối với doanh nghiệp

# Ứng phó với rủi ro trong hiện tại và tương lai

Mặc dù các nhà lãnh đạo doanh nghiệp nhận ra giá trị của việc xác minh và bảo vệ dữ liệu kinh doanh, dữ liệu và trí tuệ doanh nghiệp thường bị bỏ qua trong quá trình đưa ra quyết định.

- Dưới 33% đáp viên nói rằng họ đã tích hợp các công cụ phân tích và trí tuệ doanh nghiệp vào mô hình hoạt động của họ.
- Chỉ có 35% đã lập bản đồ cho dữ liệu của họ, có nghĩa là họ biết dữ liệu đến từ đâu và được sử dụng thế nào. Điều này tương tự cho các đáp viên có quy trình trưởng thành về giảm thiểu dữ liệu.

**Niềm tin về dữ liệu (Data trust) chưa phổ biến**

Dữ liệu là tài sản mà kẻ tấn công mạng mong muốn nhất. Doanh nghiệp có thể giảm thiểu rủi ro đó bằng cách giảm mục tiêu. Trước tiên, doanh nghiệp cần thiết lập nền tảng dữ liệu mà chúng tôi gọi là “data trust”: đảm bảo dữ liệu chính xác, được xác minh và bảo mật để từ đó, doanh nghiệp có thể sử dụng và đưa ra quyết định kinh doanh. Tuy nhiên, chỉ có khoảng một phần ba đáp viên báo cáo họ có các quy trình data trust trưởng thành, được thực hiện đầy đủ trong bốn khía cạnh chính: quản trị, khám phá, bảo vệ và giảm thiểu.

**Data trust còn chưa phổ biến**

Phần trăm số đáp viên nói rằng họ đã thực hiện đầy đủ các quy trình chính thức liên quan đến data trust


Câu hỏi: Với các tiêu chí sau, đánh giá mức độ trưởng thành data trust của doanh nghiệp bạn. Tỷ lệ phần trăm là cho các câu trả lời “có quy trình chính chính thức, được thực hiện đầy đủ”.
Cơ sở: 3,602 người trả lời
Nguồn: PwC, Khảo sát niềm tin số toàn cầu, tháng 10 năm 2021

# Sử dụng hoặc mất dữ liệu

Những phát hiện của năm nay cho thấy các quản lý cấp cao sử dụng chưa đầy đủ dữ liệu và thông tin cho quá trình đưa ra quyết định và quản lý rủi ro.

- Chỉ 30% xem xét tích hợp thông báo rủi ro trong thời gian thực vào mô hình hoạt động của họ.
- Chỉ 26% sử dụng dữ liệu để hỗ trợ định lượng rủi ro mạng, mô hình hóa mối đe dọa, xây dựng kịch bản và phân tích dự đoán - tất cả các công nghệ quan trọng cho các quyết định an ninh mạng thông minh.
- Ít hơn 30% được hưởng lợi từ các công cụ và phương pháp tiếp cận thông minh tiên tiến ngày nay như nền tảng chia sẻ thông tin với ngành công nghiệp, v.v.

Các doanh nghiệp dự đoán sẽ gia tăng chi tiêu cho an ninh mạng trong năm tới thường sử dụng các phân tích dữ liệu và trí tuệ doanh nghiệp trong mô hình hoạt động. Dữ liệu không chỉ hỗ trợ doanh nghiệp chi tiêu ngân sách mạng một cách hợp lý mà còn có thể mang lại nhiều ngân sách hơn. “Nhóm cải thiện nhất” (10% đứng đầu về kết quả an ninh mạng) có khả năng cao hơn 18 lần tuyên bố rằng những phương pháp trên là không thể thiếu trong mô hình hoạt động của họ.

# Những điểm đáng lưu ý

Dự đoán về mối đe dọa trong năm 2022

Các mục tiêu hàng đầu (dự kiến):
- Di động,
- Internet vạn vật
- Đám mây

Các loại tấn công sẽ có sự gia tăng đáng kể
- Các cuộc tấn công dịch vụ đám mây (22%)
- Mã độc tống tiền (Ransomware) (21%)
- Đào tiền ảo (crypto) (21%)

**CFO**

- Làm việc với CISO, lưu ý tới rủi ro và triển vọng tăng trưởng khi thành lập ngân sách bảo mật
- Tham khảo ý kiến của CISO về chi phí phải trả cho vi phạm và sự cố, cũng như chi phí khi ngăn ngừa những rủi ro đó.

**CISO**

- Xây dựng nền móng data trust vững chắc: Một cách tiếp cận toàn doanh nghiệp nhằm quản trị, khám phá, bảo vệ và tối thiểu hóa dữ liệu.
- Tạo một lộ trình từ định lượng rủi ro mạng đến báo cáo rủi ro mạng thời gian thực.
- Đừng dừng lại ở rủi ro mạng. Gắn liền các rủi ro mạng với các rủi ro doanh nghiệp và với những ảnh hưởng tới toàn doanh nghiệp.
- Với bản kế toán chi tiết về rủi ro mạng, hãy xác định những phương pháp phù hợp với mô hình doanh nghiệp mình và những linh vực có thể đơn giản hóa.

# Nhận biết về rủi ro

# từ bên thứ ba và chuỗi cung ứng

# Nhận biết về rủi ro từ bên thứ ba và chuỗi cung ứng

Hầu hết các đáp viên gặp khó khăn trong việc phát hiện rủi ro của bên thứ ba - những rủi ro bị che khuất bởi sự phức tạp của quan hệ đối tác kinh doanh và mạng lưới nhà cung cấp của họ. Khảo sát của chúng tôi nhấn mạnh rằng **rủi ro mạng của bên thứ ba là một điểm mù rõ ràng**:

- Chỉ có **40%** đáp viên nói rằng họ hiểu rõ ràng nguy cơ vi phạm dữ liệu thông qua các bên thứ ba và chỉ có **37%** hiểu biết về rủi ro đám mây dựa trên quy trình đánh giá chính thức.
- 56% dự kiến sự gia tăng các sự cố vào năm 2022 từ các cuộc tấn công vào chuỗi cung ứng phần mềm, nhưng chỉ có 34% đã chính thức đánh giá doanh nghiệp của họ đối với rủi ro này.

Ngày nay, mục tiêu của các tấn công mạng phổ biến có thể đến từ chuỗi cung ứng của các nhà cung cấp và các nhà thầu. Mặc dù đã phòng thủ không gian mạng tốt nhưng doanh nghiệp có thể dễ bị tấn công chuỗi cung ứng khi những kẻ tấn công chỉ đơn giản là tìm ra con đường mới xâm nhập vào doanh nghiệp thông qua các nhà cung cấp. Vậy làm thế nào để phòng thủ? Một quá trình mà nhiều người cho là đương nhiên: cập nhật phần mềm. Các tổ chức có kết quả an ninh mạng tốt nhất trong hai năm qua đã hợp nhất các nhà cung cấp công nghệ. Giảm thiểu số lượng các nhà cung cấp công nghệ và các bên thứ ba sẽ làm giảm độ phức tạp và tăng khả năng nhận biết mức độ an toàn của chúng.

**Rủi ro mạng phát sinh từ các bên thứ ba và chuỗi cung ứng là điểm mù lớn đối với các doanh nghiệp**


Câu hỏi: Mức độ hiểu biết trong doanh nghiệp về các rủi ro mạng và quyền riêng tư phát sinh từ các bên thứ ba hoặc các nhà cung cấp trong các lĩnh vực sau đây?
Cơ sở: 3,602 người trả lời
Nguồn: PwC, Khảo sát niềm tin số toàn cầu, tháng 10 năm 2021

# Những điểm đáng lưu ý

Một số giải pháp góp phần giảm thiểu rủi ro:

- Giảm số lượng bên thứ ba,
- Tăng cường quá trình giám sát
- Đánh giá chuyên sâu đối với các bên thứ ba

**COO và quản lý cao cấp chuỗi cung ứng**

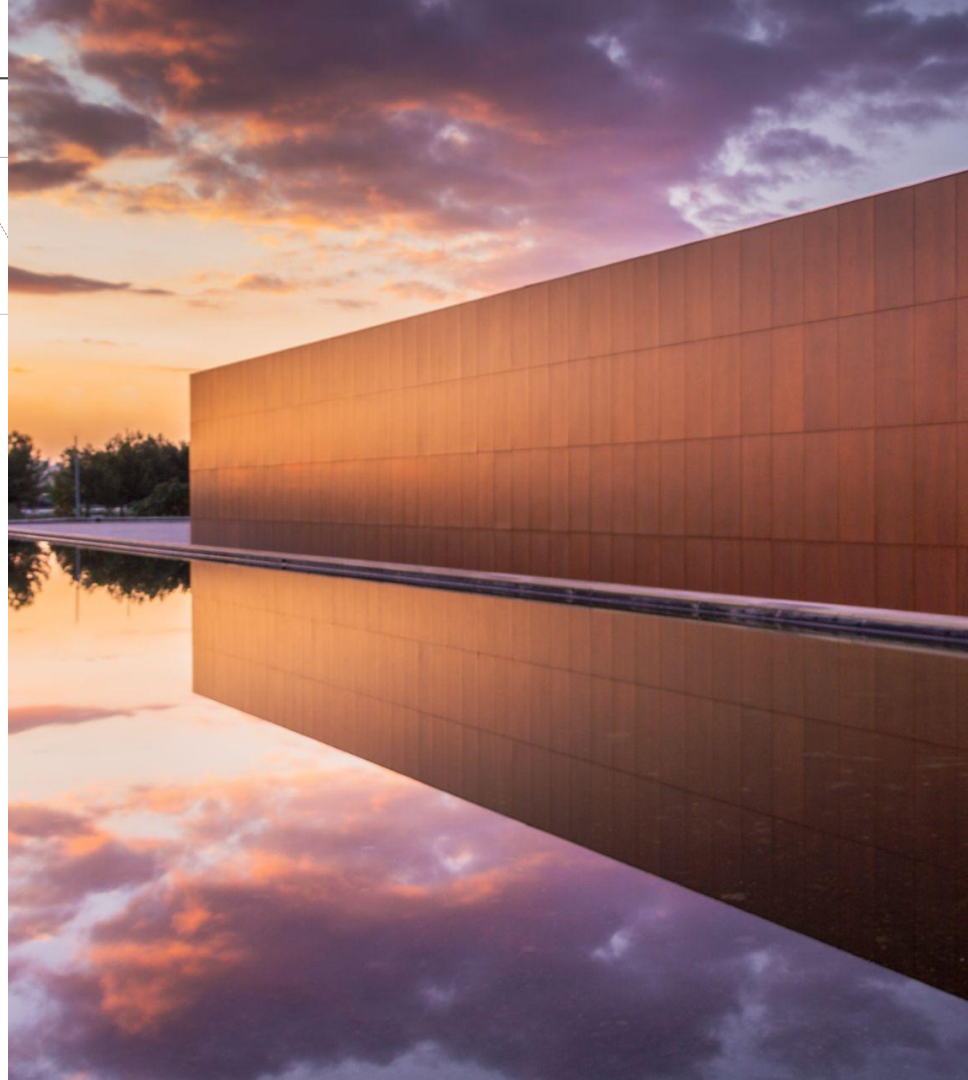
- Lập bản đồ hệ thống, đặc biệt là các mối quan hệ quan trọng và sử dụng trình theo dõi bên thứ ba để tìm ra các liên kết yếu nhất trong chuỗi cung ứng
- Đánh giá kỹ lưỡng các nhà cung cấp phần mềm so với các tiêu chuẩn hiệu suất doanh nghiệp mong đợi. Phần mềm và các ứng dụng mà doanh nghiệp sử dụng cũng cần được đánh giá kĩ càng như khi kiểm tra của các thiết bị mạng và người dùng.
- Sau khi có bản kế hoạch đầy đủ về rủi ro của bên thứ ba và chuỗi cung ứng, hãy xác định các phương pháp đơn giản hóa mối quan hệ kinh doanh và chuỗi cung ứng. Doanh nghiệp có thể quyết định nên giảm bớt hay kết hợp?

**Giám đốc quản lý rủi ro (CRO) và CISO**

- Xây dựng khả năng công nghệ nhằm phát hiện, chống lại và ứng phó các cuộc tấn công mạng thông qua phần mềm doanh nghiệp và tích hợp các ứng dụng để có thể quản lý và bảo vệ chúng một cách đồng nhất.
- Thiết lập phòng ban quản lý rủi ro của bên thứ ba để điều phối các hoạt động của tất cả các chức năng quản lý rủi ro của bên thứ ba.
- Tăng cường quy trình data trust. Dữ liệu là mục tiêu của hầu hết các cuộc tấn công vào chuỗi cung ứng.
- Giáo dục hội đồng quản trị về rủi ro mạng và kinh doanh từ các bên thứ ba và chuỗi cung ứng.

Tại Việt Nam, rất ít công ty có thể tuân thủ các yêu cầu liên quan đến chuyển đổi kỹ thuật số, đặc biệt là các yêu cầu về bảo vệ dữ liệu cá nhân và rủi ro an ninh mạng từ bên thứ ba. Do đó, việc áp dụng các tiêu chuẩn và thông lệ của quốc tế là điều cấp thiết đối với các tổ chức để nâng cao hiệu quả quản lý chuỗi cung ứng và giảm thiểu rủi ro bên thứ ba."

**Ông Phó Đức Giang**
Giám đốc
Công ty TNHH Dich vụ An toàn Thông tin
PwC Vietnam

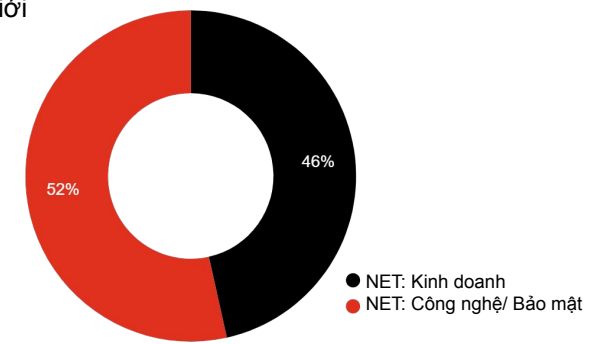


# Phụ lục

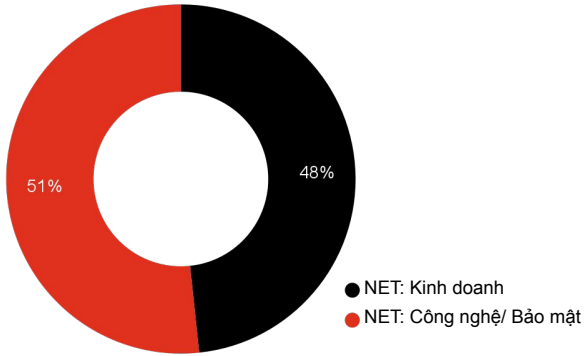
## Thông tin đáp viên

# Thông tin đáp viên

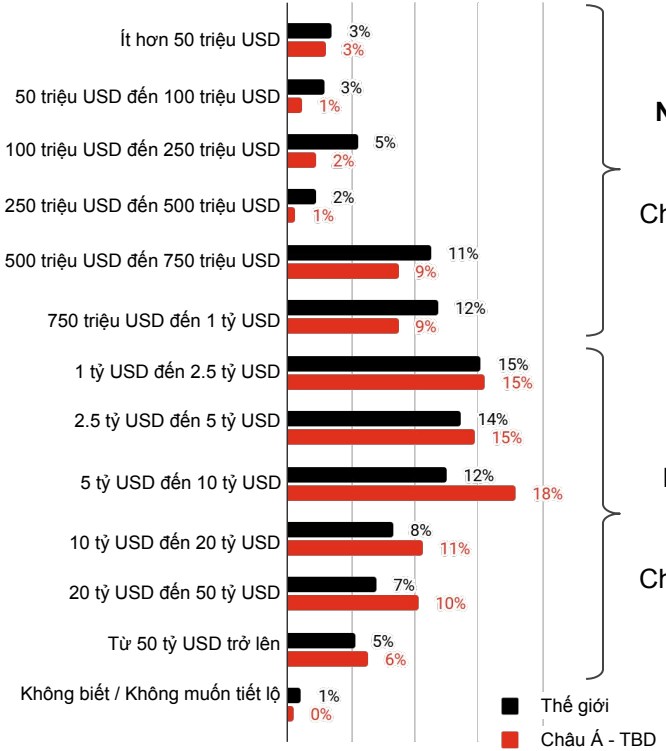
Nghề nghiệp
Thế giới




Châu Á - TBD




Thu nhập




**NET: Ít hơn 1 tỷ USD**
Thế giới: 37%
Châu Á - TBD: 24%

**NET: Lớn hơn 1 tỷ USD**
Thế giới: 62%
Châu Á - TBD: 75%

Nguồn: Khảo sát niềm tin số toàn cầu 2021, Tháng 9 năm 2021. Cơ sở: Thế giới=3602, Châu Á - TBD=633

# Nhân khẩu học

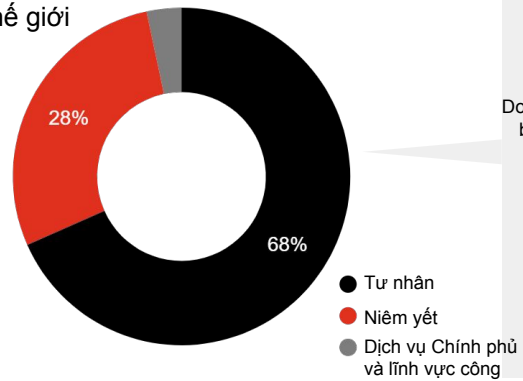
## Giới tính

**Nữ**
Thế giới: 33%
Châu Á - TBD: 27%

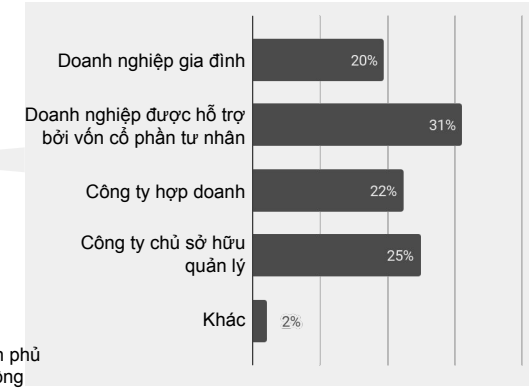
**Nam**
Thế giới: 66%
Châu Á - TBD: 62%

## Quyền sở hữu

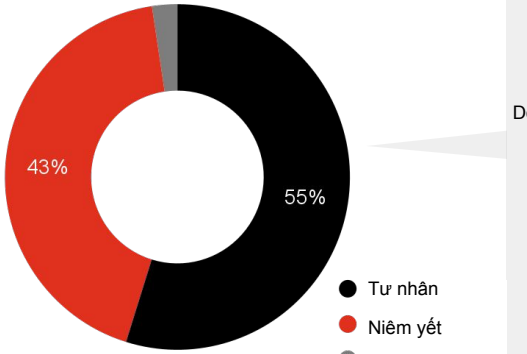
### Thế giới

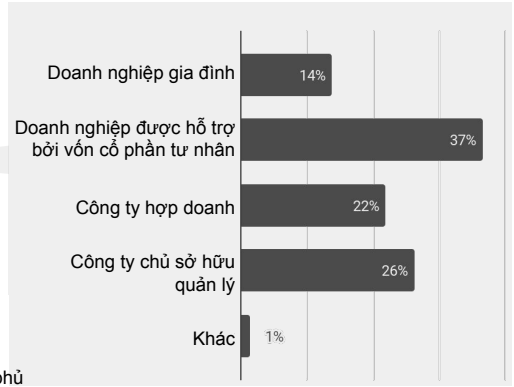



### Tổ chức tư nhân




### Châu Á - TBD




Nguồn: Khảo sát niềm tin số toàn cầu 2021, Tháng 9 năm 2021. Cơ sở: Thế giới=3602, Châu Á - TBD=633. Cơ sở của Tổ chức tư nhân: Thế giới=2462, Châu Á - TBD=347

# Liên hệ

**Bà Nguyễn Phi Lan**
Phó Tổng giám đốc, Lãnh đạo dịch vụ
Tư vấn Quản lý Rủi ro
PwC Việt Nam

**Ông Phó Đức Giang**
Giám đốc
Công ty TNHH Dich vụ An toàn Thông tin
PwC Vietnam

# Xin cảm ơn!

pwc.com/vn