



Thưa Quý Công ty,

Ngày: **05/11/2019**

Trong thời đại Cách mạng 4.0, các công ty Việt Nam, đặc biệt là các nhà cung cấp dịch vụ Công nghệ Thông tin (IT) đang có cơ hội hội nhập và gia tăng vị thế của mình trong chuỗi cung ứng toàn cầu. Khi ngành IT cùng môi trường An ninh mạng (Cyber) đang thay đổi với tốc độ chóng mặt, các nhà cung cấp dịch vụ IT cần có sự chuẩn bị tương đương với các khách hàng tập đoàn toàn cầu của mình trong việc đối phó với **những rủi ro mới về an ninh mạng và trách nhiệm nghề nghiệp** để tận dụng tối đa những cơ hội hội nhập này.

Địa điểm:
Phòng Hội nghị Quang Trung, QTSC Building 1,
Công viên Phần mềm
Quang Trung, Phường
Tân Chánh Hiệp, Quận 12,
TPHCM

Các tập đoàn lớn đa quốc gia đang ngày càng lo ngại những rủi ro tấn công an ninh mạng đến từ chuỗi cung ứng ngày một toàn cầu và phức tạp và việc phải phụ thuộc vào các bên thứ ba trong chuỗi cung ứng:

1. Những kẻ hở trong an ninh hệ thống của các nhà cung cấp có thể trở thành “cửa sau” để tin tặc tấn công mạng lưới liên kết của cả chuỗi giá trị.
2. Rủi ro gián đoạn và thiệt hại kinh doanh đến từ gián đoạn hoạt động của các công ty trong chuỗi cung ứng do nguyên nhân tấn công an ninh mạng đang ngày một trở nên thường xuyên hơn

Do đó, các tập đoàn sẽ chú trọng gia tăng kiểm soát và đảm bảo tình trạng an ninh mạng của các nhà cung cấp của mình (“**cyber due diligence**”), đặc biệt là các nhà cung cấp dịch vụ công nghệ thông tin. Các nhà cung cấp dịch vụ cũng cần chuẩn bị sẵn sàng cho tình huống bị khách hàng tập đoàn **yêu cầu bồi thường** nhằm bù đắp cho thiệt hại tài chính do sự cố an ninh gây ra.

Ngoài rủi ro an ninh mạng, khi phụ thuộc ngày càng nhiều vào dịch vụ bên thứ ba, các tập đoàn lớn cũng theo dõi sát sao hơn “**trách nhiệm chuyên nghiệp**” của các nhà cung cấp. Đặc biệt là với các nhà cung cấp dịch vụ công nghệ thông tin do mức độ phức tạp và chuyên môn, kiến thức trong dịch vụ. Rủi ro kiện tụng/ khiếu nại đòi bồi thường có thể đến từ nhiều tình huống, bao gồm nhưng không giới hạn: không đáp ứng được tiêu chuẩn dịch vụ, không thực hiện theo quy trình được thỏa thuận, các lỗi vô ý, v.v... Dịch vụ IT càng trở nên hiện đại và phức tạp thì nguồn gốc cho rủi ro trách nhiệm chuyên nghiệp gia tăng càng nhanh.

Cung cấp dịch vụ cho các khách hàng quy mô càng lớn thì rủi ro càng cao, các công ty cung cấp dịch vụ công nghệ thông tin cần chủ động hơn trong chiến lược quản lý rủi ro an ninh mạng và kiện tụng/ khiếu nại của mình.

Hội thảo “**Rủi ro Trách nhiệm Chuyên nghiệp & An ninh Mạng của Công ty Công Nghệ khi tham gia Chuỗi Cung ứng Toàn cầu**” được thực hiện với mục tiêu giúp Quý Công ty hiểu rõ hơn về bức tranh toàn cầu mà chúng ta đều đang tham gia hội nhập, và đảm bảo rằng công ty mình đang thực hiện các biện pháp tự bảo vệ trong hệ sinh thái “cyber” thế giới.

Chúng tôi hy vọng Hội thảo này sẽ mang lại những thông tin cần thiết giúp Quý Công ty gia tăng sức cạnh tranh của doanh nghiệp mình, với tư cách là nhà cung cấp đáng tin tưởng trong chuỗi cung ứng quốc tế.

Trân trọng,

Thời gian

14:00 – 14:30: Đón tiếp
14:30: Rủi ro Trách nhiệm liên quan đến An ninh Mạng của các nhà cung cấp dịch vụ IT – Aon
15:30: Nghỉ giữa giờ
15:45: Những Rủi ro Trách nhiệm Nghề nghiệp mới phát sinh của ngành IT Toàn cầu – QBE
16:30: Hỏi đáp Thảo luận
17:00: Bế mạc Hội thảo

Vui lòng đăng ký tham dự tại [đây](#)

Thông tin Diễn giả

Andrew Mahony – Giám đốc, Giải pháp Rủi ro An ninh Mạng, Aon Châu Á

Andrew là chuyên gia trong lĩnh vực rủi ro không gian mạng, rủi ro tài chính và trách nhiệm nghề nghiệp, đặc biệt chuyên về nghiên cứu rủi ro an ninh mạng và đánh giá hiệu quả chương trình bảo hiểm (tư vấn điều kiện điều khoản). Andrew có kinh nghiệm làm việc với nhiều thương hiệu tên tuổi lớn có rủi ro an ninh mạng phức tạp nhất trong khu vực Châu Á. Andrew được công nhận là một trong số những chuyên gia nghiên cứu hàng đầu về rủi ro an ninh mạng trong khu vực, với nhiều bài viết, phỏng vấn với các kênh truyền hình ChannelNewsAsia, Al Jazeera và BBC. Ông cũng đã trình bày tại Hội nghị thường niên PARIMA, MAS FinTech Festival, và sự kiện thường niên Aon Insights Series về bức tranh rủi ro an ninh mạng biến đổi không ngừng và xu hướng phát triển đáp ứng của thị trường bảo hiểm.

Sara Kobes – Chuyên gia, Giải pháp Rủi ro An ninh Mạng, Aon Châu Á

Sara hiện đang làm việc với nhiều công ty lớn trong khu vực châu Á về rủi ro An ninh mạng, tham gia thực hiện huấn luyện, đào tạo cho các khách hàng quốc tế trong khu vực. Sara có nhiều kinh nghiệm trong việc hỗ trợ các tập đoàn có hoạt động, nền tảng và đặc điểm đa dạng, giúp các công ty này quản lý rủi ro an ninh mạng trong môi trường rủi ro biến đổi năng động.

Ronak Shah – Giám đốc Khu vực, Bộ phận Tài chính, Trách nhiệm Nghề nghiệp - QBE Châu Á

Ronak có hơn 19 năm kinh nghiệm trong ngành bảo hiểm tại ba công ty môi giới bảo hiểm toàn cầu và một trong số những công ty bảo hiểm lớn nhất, ở thị trường Mỹ và Singapore. Kinh nghiệm của ông bao gồm thiết kế và thu xếp bảo hiểm Tài chính, Trách nhiệm Chuyên nghiệp cũng như Trách nhiệm trong hoạt động Giao dịch bao gồm Trách nhiệm An ninh Mạng, Trách nhiệm Hành nghề Y, Thử nghiệm Lâm sàng, Trách nhiệm Ban Giám đốc & Người điều hành, Trách nhiệm Sản phẩm, Trách nhiệm Môi trường, Trách nhiệm chung, Trách nhiệm Đại diện, bảo hành và thuế, v.v....

Ronak tham gia đóng góp với vai trò ý kiến chuyên gia cho nhiều tạp chí kinh tế tài chính, và là diễn giả thường xuyên tại các hội thảo, thực hiện huấn luyện, đào tạo cho nhiều tập đoàn lớn trong khu vực. Ông hiện đang là Chủ tịch của Hiệp hội PLUS ở Singapore. Ronak có Bằng Cử nhân Khoa học về Kỹ thuật Điện và Máy Vi tính và Cử nhân Kinh tế tại trường đại học Rochester, Hoa Kỳ.