La gran entrevista - Líder de riesgo cibernético Ramy Houssaini



Ramy Houssaini ha liderado privacidad y riesgo cibernético para una de las multinacionales bancarias más grandes del mundo desde 2017, una posición con una responsabilidad estratégica significativa, pero comenzó su carrera en la cara del carbón desarrollando software no frágil para una infraestructura de telecomunicaciones altamente resistente en Motorola.

Ese rol "me dio la oportunidad de colaborar estrechamente con los equipos de productos de ingeniería y operaciones", recuerda. Tender un puente entre los mundos de los negocios y la tecnología ha sido su oficio desde entonces: "Siempre he estado en roles en los que actué como esa capa de traducción entre lo que eran los requisitos y estrategias comerciales; y luego cuáles deberían ser los controles de ingeniería reales y las consideraciones de infraestructura ... Al principio de mi carrera, consideré que el "ciberespacio" no existe de forma aislada; se trata de la habilitación empresarial", señala, y agrega que "probablemente la computadora más segura [después de todo] es una apagada que no sirve para ningún propósito comercial".

Cuando se le preguntó si este "puente" se ha vuelto más fácil a lo largo de los años, a medida que la forma en que la tecnología puede mover la aguja comercial, y una conciencia más amplia del riesgo cibernético, se elevan en la junta y la agenda de la C-Suite, se le ocurre una respuesta considerada, pero un poco inesperada: "En realidad siento que ha habido más esfuerzo de la comunidad empresarial; líderes de producto y estrategas, CEOs, la junta directiva para entender el mundo de la tecnología... que los tecnólogos realmente [haciendo ese esfuerzo para entender] cuál es su contexto empresarial, y tratando de formular realmente las estrategias arquitectónicas adecuadas para apoyar eso", reflexiona en un Zoom \* con [*The Stack*](https://thestack.technology/).

"Hay, por supuesto, algunos sectores y algunos entornos donde existe esa simbiosis y es un equilibrio perfecto. Pero si tuviera que hablar en términos agregados, creo que ahora se ve que las salas de juntas y los equipos de gestión se sienten más cómodos hablando de tecnología. Pero si va a sus organizaciones tecnológicas típicas, todavía tiene una visión insular de la función. Y eso", subraya con firmeza, "tiene que cambiar..."

Ramy, que se casa de manera afable con lo que es claramente una mentalidad centrada en las operaciones cuando se trata de riesgo, datos y seguridad, ha trabajado en ciberseguridad durante dos décadas, con períodos como líder de práctica de seguridad para BT Global Services y jefe de la práctica de ciberseguridad en Accenture. (Siguió su primer título en ingeniería informática y eléctrica en la Universidad McGill con una maestría en gestión de sistemas de información en Northwestern, luego un MBA en la Universidad de Duke). Como él dice, "he sido educativo para obtener perspectivas de diferentes industrias. Me ayudó a redondear mis pensamientos, pero también a adquirir algunas cicatrices de batalla".

Cicatrices o no, claramente disfruta del trabajo: "Mi parte favorita de este trabajo es la comunidad unida y la colaboración multifuncional, incluso entre empresas competitivas. Las relaciones y la camaradería realmente hacen que el trabajo sea satisfactorio y crea amistades duraderas. Otro aspecto que me encanta de esta carrera es que cada mañana, cuando te levantas, sucede algo nuevo. Los [TTP](https://www.mitre.org/publications/technical-papers/ttp-based-hunting) que usan los hackers no han cambiado drásticamente en la última década, pero las superficies de ataque, la forma en que se aplican las técnicas siempre está evolucionando".

**Ramy Houssaini: Mis 3 prioridades principales para 2022**

Aunque el trabajo puede ser satisfactorio, también puede ser intensamente exigente. El agotamiento es cada vez más frecuente en toda la industria, al igual que la rotación. Pase más de cinco minutos en Twitter y se encontrará con un profesional de la seguridad de la información que sueña con convertirse en agricultor, artista o cualquier otro rol que no involucre computadoras.

Cuando se le preguntó cuáles son sus tres prioridades para 2022, esas presiones son algo sobre lo que se apresura a reflexionar.

"Mi primera prioridad es cuidar a mi equipo", responde:

"Una de mis ideas duraderas de los últimos dos años es que, si bien todos estamos en la misma tormenta, no todos estamos en el mismo barco. Puede parecer que estamos en la misma crisis, pero las realidades y demandas de esta crisis son muy diferentes para cada individuo. Tenemos que seguir recordándonos a nosotros mismos que cada uno tiene necesidades diferentes. Así que un enfoque clave para mí es cómo entender mejor el costo mental y físico que los últimos dos años han creado para el equipo y crear las condiciones para que todos se recuperen y prosperen.

"Mi segunda prioridad es estar cerca de lo que está cambiando con el aumento de la adopción de servicios en la nube. A medida que las API y la tecnología en la nube se vuelven más interoperables, debemos descubrir cómo aprovechar la automatización y convertir el programa de seguridad en servicios que simplemente se integren en estos entornos tecnológicos en lugar de centrarse en las inspecciones manuales. Y mi tercera prioridad es dar forma a las experiencias de los clientes del futuro:reducir la complejidad y mejorar la usabilidad de los controles / guardias ferroviarios al tiempo que permite una experiencia mejorada para los clientes internos y externos. Esto también significa convertir la ciberseguridad y la privacidad en un generador de valor para la empresa..."

**Los retos más difíciles...**

La rápida evolución del ámbito cibernético crea algunas complicaciones. Él elige dos desafíos clave.

"Uno de los principales desafíos a los que se enfrentan los equipos de ciberseguridad hoy en día es la mayor complejidad asociada con la operación y gestión de una multitud de controles de seguridad. Esto es difícil por dos razones: primero, la telemetría generada por los diversos controles crea ruido que requiere un procesamiento significativo para capturar las señales débiles clave y filtrar los falsos positivos. Esto puede explicar, por ejemplo, cómo algunas violaciones profundas recientes tardaron un tiempo antes de que las señales iniciales detectadas condujeran a una confirmación clara del ataque.

"En segundo lugar, la proliferación de soluciones puntuales obliga a la especialización de la fuerza laboral de ciberseguridad y limita su comprensión de extremo a extremo de la postura de ciberseguridad de la organización", dice.

"En este contexto", señala por correo electrónico, "la optimización de la matriz de controles y su alineación con una arquitectura de seguridad clara se vuelve más desafiante. El impacto posterior es un aumento significativo e insostenible de los costos operativos de seguridad y la pérdida de un enfoque basado en el riesgo en la gestión de la ciberseguridad.

"El otro desafío que se ha visto amplificado por la reciente pandemia es la necesidad de reinventar el modelo operativo de ciberseguridad para dar cuenta de una expansión en la huella digital de una organización y las limitaciones de realizar actividades clave de ciberseguridad (por ejemplo. forenses) en condiciones inusuales. Estos cambios inducirán una re-orquestación de las capacidades (más distribuidas) y un replanteamiento de la cadena de suministro de seguridad para introducir más dependencias de los proveedores externos. Esto en sí mismo aumenta aún más la importancia de mejorar la gestión del riesgo cibernético de terceros y adoptar un enfoque más impulsado por el ecosistema", algo, señala, que "sigue siendo difícil incluso para las organizaciones más maduras". (Particularmente a medida que el riesgo de la cadena de suministro de software continúa creciendo).

**La seguridad como habilitador...**

"Filosóficamente", agrega, sin embargo, "la seguridad nunca debería estar en condiciones de decir 'no'.

"Resolver un problema de seguridad es fundamentalmente un desafío de ingeniería. Se trata de demostrar realmente el arte de lo posible; se trata de proponer enfoques innovadores, y no necesariamente aplicar mecánicamente una lista de verificación y aprovechar la lista de verificación para decir: "este control en particular contradice esta configuración particular y, por lo tanto, la respuesta es no". Tal vez no estamos haciendo las preguntas correctas, tal vez haya una innovación en términos de un enfoque interesante para abordar el requisito fundamental, al tiempo que cumplimos con los controles a los que nos gustaría adherirnos. Así que creo firmemente en la necesidad de no adoptar un enfoque de lista de verificación cuando se trata de seguridad, sino que realmente piense en cada desafío como un problema de ingeniería.

"Eso significa implementar algo de ingenio y encontrar la solución adecuada. Cuando se trata de privacidad, ahora tenemos algunas innovaciones muy interesantes en tecnologías que permiten la privacidad que nos permiten mantener ciertos flujos, al tiempo que garantizamos la confidencialidad y la integridad de la información. Realmente depende de nosotros aprovechar estas tecnologías a nuestro favor y encontrar formas de decir 'sí', más a menudo".

Presionado por un ejemplo duro, menciona los datos sintéticos, como uno, señalando: "Muchos problemas se pueden resolver aprovechando a veces los datos sintéticos. Y [sin embargo] la adopción de datos sintéticos sigue siendo muy baja en muchos entornos. Puede abordar las limitaciones en torno a la I + D y la innovación aprovechando dichos datos.

"Y si queremos asegurarnos de que estamos reduciendo el riesgo de duplicación de datos; que tenemos muy claro cuáles son los inventarios de activos, somos capaces de hacer cumplir las cosas de una manera más natural y menos compleja [tenemos que pensar en] la usabilidad de los controles. Eso se relaciona con algo realmente importante: la experiencia del cliente. ¿No deberíamos pensar en qué hacemos de forma aislada de cómo el cliente está experimentando ese producto en particular? ¿Y cómo podemos hacer que la seguridad se convierta en un control ambiental, en lugar de algo en el camino?"

**Desmitificando la seguridad para la sala de juntas**

Pensar en la experiencia del cliente es importante. También lo está la junta y Ramy Houssaini ha estado profundamente involucrado en el establecimiento de un nuevo programa de capacitación para los miembros de la junta sobre ciberseguridad, que está siendo dirigido por el Instituto DCRO, una organización sin fines de lucro que aporta experiencia esencial en gobernanza de riesgos a la sala de juntas y la C-suite.

"El ciberespacio es como cualquier otro riesgo empresarial", explica a The Stack. "El riesgo cibernético es un panorama en evolución y cambia con la actividad de fusiones y adquisiciones, [la] introducción de nuevos productos / capacidades al mercado ... Los miembros de la junta hoy en día deben comprender este uso estratégico de la tecnología y asegurarse de que el equipo de gestión esté implementando adecuadamente la tecnología para permitir que el negocio tenga éxito al tiempo que puede traducir el riesgo cibernético y los datos complicados que se encuentran debajo de él en decisiones de riesgo comercial. Para que esto suceda, deberán estar equipados con el conocimiento y la comprensión adecuados de los problemas. Esta es la visión del [programa](https://courses.dcroi.org/courses/cyber-risk-governance)".

**¿Los mejores consejos para compañeros?**

¿Qué más ha aprendido en su viaje hasta la fecha sobre la construcción de programas de seguridad sólidos?

"Yo diría que invierta en Inteligencia procesable basada en una arquitectura de seguridad clara y no en balas de plata de seguridad", dice, aclarando que "por Inteligencia no me refiero necesariamente a inteligencia de amenazas, sino más bien a la comprensión mejorada general de la postura de ciberseguridad y la capacidad de hacer una mejora clara y medible en la ciber resiliencia. Esto generalmente requiere la integración y el análisis de varias señales y la racionalización de las herramientas para garantizar que los controles obsoletos, que generalmente son una fuente de distracción y sobrecarga operativa, se eliminen gradualmente en favor de otros más efectivos. El requisito previo para esto es tener una arquitectura de seguridad bien articulada y la hoja de ruta de tecnología asociada.

"Tener la disciplina de invertir el tiempo para estudiar cuidadosamente el entorno y diseñar controles adecuados para el propósito en lugar de cubrir la organización con controles ineficaces pagaría dividendos. Los proveedores [también] necesitan comprender el contexto de su posible cliente y los principios que guían su arquitectura de seguridad para luego posicionar su solución / plataforma en alineación y ofrecer los beneficios adyacentes, como reemplazar una pila completa de controles existentes, permitir una seguridad sin fricciones y mejorar la calidad de las decisiones que los CISO y los equipos de ingeniería de seguridad podrían estar tomando para mejorar la postura cibernética de sus organizaciones. Se debe hacer hincapié en cómo las plataformas permiten las acciones y cómo se integran en el tejido operativo".

**Construyendo un equipo de seguridad fuerte...**

En última instancia, una postura de riesgo de seguridad mejorada es un deporte de equipo, enfatiza Ramy Houssaini: "La densidad de habilidades de ciberseguridad en toda la empresa es más importante que el número de personas en la organización de seguridad. Esta es una consideración de diseño importante para un equipo de seguridad que reconoce que la seguridad es un deporte de equipo que requiere la participación de varias partes interesadas en los equipos de productos, ingeniería, operaciones, funciones de control y el negocio. En la práctica, significa garantizar que el equipo de seguridad ampliado se examine de manera integral para comprender las capacidades existentes y las que requieren reconstrucción / revitalización.

"En cuanto a la configuración de los equipos, debe haber un equilibrio entre las responsabilidades operativas, las de asesoramiento y las de gestión y control de riesgos. Esto tiene implicaciones en la diversidad de los perfiles necesarios para garantizar una cobertura de espectro completo para las responsabilidades multidimensionales de la organización de ciberseguridad. Una consideración importante es adoptar una orientación basada en servicios. Los equipos deben estructurarse sobre la base de un catálogo de servicios claro que codifique las expectativas y los resultados, así como el compromiso y la colaboración necesarios con otras partes interesadas. Esto mejorará aún más la claridad de los equipos sobre sus objetivos y también permitirá a los socios externos comprender mejor los diferentes modelos de compromiso".

Esto está a un mundo de distancia de algunos de los programas de seguridad altamente reactivos que a veces proliferan en las grandes organizaciones. ¿Dónde y cómo tiene tiempo para dar un paso atrás de la ráfaga de tareas diarias que todos tenemos y asegurarse de que está pensando estratégicamente sobre cómo se estructuran los equipos y las arquitecturas?

Su respuesta suena ligeramente apologética, como si hubiéramos esperado que estuviera haciendo algo esotérico con una Raspberry Pi: "En realidad me gusta la jardinería... Creo que tratamos con muchos conceptos abstractos [en el trabajo]. Y a veces es importante encontrar algo de cordura al hacer algo en lo que pueda ver resultados más inmediatos de inmediato. La jardinería me aporta serenidad. Esa es mi forma de manejar el estrés, pero también una pasión.

Y con eso se va a poner bajo la manga: ya sea para cultivar un árbol frutal o un proyecto de datos, siempre tratando de abordar el resultado con un diseño y una arquitectura claros en mente.

*\*La entrevista incluyó una llamada de Zoom, así como preguntas escritas. Hemos extraído de ambos para este artículo.*

