Gestión de crisis en un caso de ransomware

Caso

“Parece que estamos bajo ataque.”

Esas fueron las palabras que Andrea Espinosa, Directora Ejecutiva de Guidaí, una empresa de Coaching Comunicacional, escuchó inmediatamente después de responder una llamada telefónica temprano en la mañana de su Director de Tecnología. "Andrea, es un ciberataque". Todas las computadoras de las oficinas de Guidaí, tanto en Montevideo como en Buenos Aires, estaban fuera de línea. Los monitores mostraban una nota de *ransomware* solicitando el pago en bitcoins, una conocida criptomoneda, sin especificar la cantidad exacta. “El precio final depende de la rapidez con la que nos contacten”, decía el mensaje.

La empresa Guidaí

Espinosa fundó Guidaí en 2016 después de cansarse de la cultura de la retroalimentación en su antiguo empleador. “La retroalimentación de los gerentes fue superficial y optimista o incisiva e hiriente. Pero sobre todo se inclinó hacia la retroalimentación negativa, que hizo metástasis en una cultura de miedo y agotamiento”, recordó. Después de iniciar Guidaí como un proyecto paralelo, Espinosa se dedicó a tiempo completo a construirla en 2017.

En 2024, Guidaí era una empresa que proveía servicios a otras empresas (B2B) y a consumidores (B2C), que se posicionó como proveedor de “gestión como servicio” (MaaS), una rama del popularizado “software como servicio” (SaaS). El producto estrella de Guidaí se centró en la comunicación de retroalimentación (*communication feedback*). Tanto las empresas como los individuos recurrieron a esta consultora para recibir capacitación sobre cómo entregar y recibir comentarios y aprovechar la retroalimentación (*feedback)* de gerentes, colegas, amigos, socios o familiares. Guidaí, que lleva el nombre por un término en Charrúa que significa "Luna”, se autodenominó como una empresa de coaching comunicacional, emocionalmente inteligente y conocedora de los negocios, cuyo objetivo es hacer que las conversaciones más importantes sean las más efectivas. En otras palabras, la consultora se especializaba en la gestión de la comunicación humana. Guidaí tenía tres valores fundamentales: cuidado, coraje y colaboración.

Después de varios años de luchas iniciales y escepticismo de los inversores, la empresa experimentó un crecimiento sustancial en 2020, en medio de una pandemia global y movimientos sociales simultáneos. Se convirtió en una de las aplicaciones móviles más descargadas en su categoría, a medida que personas de todo el mundo enfrentaban conversaciones difíciles y las organizaciones buscaban formas de apoyar a los empleados.

La incorporación de clientes se disparó tras varios artículos en publicaciones especializadas y las apariciones de Espinosa en medios de comunicación. Si bien el reconocimiento público y el crecimiento de clientes fueron notorios, Espinosa sabía que Guidaí aún no había alcanzado su potencial. Quería aprovechar su nueva posición en el mercado para recaudar la ronda de financiamiento más grande de su historia en los mercados privados, lo que le permitiría ampliar su oferta y extender su crecimiento, particularmente en las categorías de coaching (por ejemplo, coaching de negociación), internacional (p. ej., comunicación intercultural) y juventud (por ejemplo, con un producto centrado en ayudar a niños y adolescentes a comunicar sus sentimientos). En este sentido, la pandemia fue para Guidaí una oportunidad única de ampliar su impacto y Espinosa estaba decidida a hacer avanzar a su empresa.

Tomado como rehén: qué significó para Guidaí

Justo antes del ciberataque, Espinosa y su equipo finalmente habían llegado a la etapa final de una nueva e importante ronda de financiamiento proveniente de capitales de riesgo. Las posibles consecuencias de la crisis de ciberseguridad de Guidaí podrían llevar no solo a los inversores a retirarse sino también, a interrumpir el crecimiento que la empresa había experimentado.

Aunque aún no se ha confirmado, sabían que los ciberdelincuentes podrían tener acceso a información confidencial: registros escritos y audiovisuales de las percepciones que las personas tienen entre sí, así como información demográfica de los usuarios, incluida su edad, sexo, raza, salario, expectativas e historial laboral. Después de todo, Guidaí ofrecía a los usuarios la posibilidad de introducir sus pensamientos o impresiones sinceros y sin filtros de ninguna naturaleza. Su inteligencia artificial ayudaba a los usuarios a formular y articular sus mensajes para una comunicación más eficaz.

Estos “diarios” de usuarios a menudo contenían detalles privados y provocativos. ¿Los ciberdelincuentes publicarían esa información si Guidaí no cooperaba (la llamada doble extorsión)? De ser así, ¿podría recuperar la confianza de sus usuarios y clientes o su marca sufriría un daño catastrófico? Para añadir a la lista de preocupaciones, la aplicación para móviles de Guidaí no funcionaba correctamente debido al *ransomware*. Sólo sería cuestión de tiempo hasta que se materializaran las quejas y consultas sobre el apagón.

La convicción de Espinosa

Al mediodía del primer día de la crisis, Espinosa había decidido no pagar ningún tipo de rescate. Había considerado la opción de pago, pero entendió que la actividad delictiva era repugnante y pagando, se convertiría en una especie de “cómplice”. En una reunión de emergencia convocada esa mañana con su equipo ejecutivo debatieron qué se debería hacer. El equipo ejecutivo incluía al Director Financiero (CFO), al Director de Operaciones (COO), a la Directora de Tecnología (CTO), al Director de Marketing (CMO), que también era responsable de desarrollo empresarial, y al/a la

directora/a de Ciberseguridad (CISO) que no pudo asistir porque estaba en el proceso de contener el incidente. ,

Al concluir la reunión, Espinosa preguntó a su equipo:

CEO: Antes de terminar, me gustaría saber su respuesta final. Vayamos uno por uno. Dígame cuál es su voto: si es a favor de pagar el rescate o si es no pagarlo, fundamentando su parecer. Teolinda, tú primero.
CTO: No pagues. De cualquier manera, estaremos muy ocupados solucionando esto. Pero pagar el rescate sólo socavará a algunos y ¿qué valores enfatizará? ¿Qué dirás? ¿Qué vas a hacer? ¿Cómo liderarás en esta crisis?

Directora Ejecutiva: Gracias, Teo. Abelardo.

CMO: Creo que deberíamos pagar. El tiempo de inactividad no me preocupa tanto como la imposibilidad de conservar la confianza de nuestros clientes en este entorno competitivo y los daños que podrían afectar nuestra reputación si no respondemos a sus demandas. Incluso si tenemos que hacer público el pago, podemos formularlo de manera que los usuarios sepan cuán seriamente los valoramos. La gente es más indulgente con una empresa (cualquier empresa) que utiliza su dinero para pagar un rescate que con una empresa que pone en peligro su propia privacidad y seguridad. Solo piensa en las demandas que podríamos enfrentar si esta violación de datos resulta en daños o perjuicios para nuestros clientes.

CEO: Gracias, Abelardo. Evaristo.

Director de Operaciones: Estoy con Teo en este caso. No pagues. Para abordar completamente este problema, necesitaremos capacitar al personal y fomentar ciertos comportamientos. Me temo que será más difícil impulsar el cumplimiento y la cooperación si aquí se desarrolla una cultura basada simplemente en pagar para que los problemas desaparezcan.

CEO: Muy bien, gracias, Evaristo. Por último, pero no menos importante, Estanislao.

Director Financiero: Pagar. Creo que primero deberíamos negociar y eventualmente pagar. Mi estimación inicial es que probablemente será menos costoso pagar el rescate. Además, podría haber sanciones de organismos reguladores, por ejemplo, si hubiera filtración de datos personales. Y lo más importante, tenemos que pensar en dónde nos encontramos en este momento. Creo que podemos lograr que los inversores acepten el pago y una resolución rápida. No sé cómo cerraremos esta ronda si nuestros sistemas no están operativos durante un período corto. Como sabes, las consecuencias de no poder recaudar dinero serían muy importantes para esta empresa.

CEO: Está bien, dividido en partes iguales, pero por diferentes razones. Resta la opinión del/de la CISO, con quien me comunicaré más tarde. Gracias a todos. Después de hablar con él/ella, necesitaré pensar un poco a solas y luego hablaré con la Junta. Denme una hora.

Espinosa salió de la reunión de emergencia y necesitó caminar. Siguió meditando los puntos de vista planteados por su equipo ejecutivo. Había múltiples partes interesadas a tener en cuenta y muchos riesgos e incertidumbres. Como fundadora y directora ejecutiva de Guidaí, pensó seriamente en los valores de la gestión: salvaguardar, promover y actuar en nombre de los intereses de la organización y de los clientes. También como parte de esa gestión, quería demostrar y reforzar los tres valores fundamentales de la empresa: cuidado, coraje y colaboración. Mientras tanto, a nivel personal, el mayor punto de presión fue la integridad. ¿Cuál sería una decisión integral en esta situación?

Antecedentes: el panorama de ciberseguridad y el *ransomware*

En 2022, el gobierno de EE. UU. consideró que el *ransomware* y las amenazas de ciberseguridad asociadas se encontraban entre los riesgos más graves que enfrentaban las organizaciones públicas y privadas y las personas. Según el *Identity Theft Resource Center*, las violaciones de datos relacionadas con *ransomware* en los Estados Unidos se habían duplicado cada año desde 2020. Se estimó que una de cada cuatro empresas *Fortune 1000* sufriría un costoso evento de ciberseguridad de este tipo por año.

Una estimación consideraba que cada 11 segundos, en algún lugar del mundo, una empresa había sufrido un ataque de *ransomware*. Desde el transporte hasta los servicios públicos, hospitales, escuelas, empresas dedicadas al envasado de carne y empresas de primera línea se habían visto afectadas. Los ataques cibernéticos se dirigieron y afectaron prácticamente a todas las industrias y sectores de la sociedad.

Grandes corporaciones como *Bank of America* gastaron más de mil millones de dólares al año en ciberseguridad, pero los directivos e investigadores enfatizaron que las organizaciones de todos los tamaños enfrentaban riesgos de este tipo. “Todas las organizaciones deben reconocer que ninguna de ellas está a salvo de ser atacada por un *ransomware*, independientemente de su tamaño o ubicación”, escribió Anne Neuberger, Asesora Adjunta de Seguridad Nacional en tecnologías cibernéticas y emergentes de los EEUU, en una carta abierta de 2021 al sector privado. Por otro lado, en una frase atribuida a distintas personas que argumentaban que todas las organizaciones deben proteger su ciberseguridad, se afirmó que existían dos tipos de empresas: las que han sido vulneradas por un ataque externo y las que aún no sabían que lo habían sido.

Las organizaciones estuvieron expuestas a diferentes tipos de ataques cibernéticos (por ejemplo, *malware*, *phishing* o *exploits* de día cero, entre otros), provocados por delincuentes de distinta naturaleza (por ejemplo, grupos delictivos patrocinados por los Estados, actores individuales, personas con información privilegiada, etc.).

Si una organización se ve impedida de acceder a sus propios sistemas o perdió el control sobre sus datos debido a un ataque de *ransomware*, normalmente se entendía que la única manera de recuperarlo era pagando el rescate. Sin embargo, la restitución no era garantía. un estudio de una reconocida empresa de ciberseguridad mostró que solo el 51% de las organizaciones que pagaron un rescate obtuvieron nuevamente el acceso a sus datos en su totalidad sin pérdida o deterioro. Además, pagar un rescate no confería inmunidad: la investigación indicó que el 80% de las organizaciones que lo hicieron fueron posteriormente atacadas nuevamente, a menudo por los mismos delincuentes. Por lo tanto, parecía que no había una salida fácil a una crisis de ciberseguridad: si una entidad no pagaba el rescate, ponía en peligro numerosas dimensiones de su negocio, desde las operaciones hasta la marca y la gestión de clientes. Si la empresa pagaba el rescate, aún podía ser vulnerable y tener que reconstruir sus sistemas internos.

En Estados Unidos, por ejemplo, las regulaciones de ciberseguridad varían en alcance. Casi la mitad de los estados tiene leyes que regulan la seguridad y la eliminación de datos. La acción a nivel federal se llevó a cabo principalmente a través de órdenes ejecutivas y agencias. Sin embargo, en marzo de 2022, el Gobierno de EE. UU. aprobó una ley que exige que las entidades del país que proveen servicios críticos informen a funcionarios federales sobre incidentes cibernéticos y pagos de rescate efectuados.

En caso de un ciberataque, se disuadió (pero no se prohibió) a las empresas estadounidenses a que pagaran rescates, aunque las transacciones con determinados actores podían exponerlas a sanciones federales. Como resultado del mosaico legal en EEUU que dejaba espacio para las prerrogativas individuales, la toma de decisiones críticas durante una crisis de ciberseguridad a menudo recaía sobre los hombros de las víctimas.

Consigna: comunicación y gestión de crisis

Imagine que usted es el/la CISO de Guidai. ¿Cuál sería su recomendación, después de conocer a través de Espinosa, las opiniones de sus pares? ¿Qué le diría a Espinosa y cómo justificaría su respuesta? Tanto si la decisión de Espinosa fuera pagar, como si fuera no hacerlo, ¿cómo cree que debería comunicarse a los distintos roles involucrados? Piense al menos en la Junta Directiva, los empleados, los inversores potenciales, los clientes, los ciberdelincuentes, las entidades reguladoras y los medios de comunicación. ¿Qué valores deberían enfatizarse con cada uno de ellos? ¿Qué acciones llevará a cabo en cada una de las dos situaciones que podrían desencadenarse a partir de la decisión de Espinosa? Puede hacer todos los supuestos que desee y agregar cualquier otra cuestión que piense puede ser de interés para el caso.