Reputación y ciberseguridad: del riesgo a la oportunidad, y el ciberorgullo

kaspersky

Reputación y ciberseguridad: del riesgo a la oportunidad, y el ciberorgullo

"Toma 20 años forjar una reputación y cinco minutos para arruinarla. Si piensa al respecto, llevará a cabo las cosas de manera diferente".
(Warren Buffett)

Los límites del miedo como motivación: comentarios desde la psicología
El miedo es útil. De acuerdo con los neurólogos del Hospital Karolinska en Estocolmo, "La función del miedo es motivar a los organismos a enfrentar las amenazas que pusieron en peligro la supervivencia a lo largo de la evolución".

Sin embargo, las respuestas de protección del miedo (paralizarse/luchar/huir) no se crearon para enfrentar los obstáculos en el lugar de trabajo moderno. La lucha tiene un papel que desempeñar en el contexto de un incidente cibernético inmediato, pero la respuesta de la lucha puede ser una solución brusca y siempre a corto plazo.

Psicóloga
Christine Tappolet (Universidad de Montreal) hace este breve comentario: "El miedo influye en lo que realizamos reduciendo el enfoque del agente (es decir, el nuestro)". Solo nos centramos en la amenaza que tenemos ante nosotros ahora mismo, a expensas de observar el panorama global.

En psicología, se distingue entre la motivación de acercamiento (la atracción por un aspecto positivo, impulsada por la esperanza) y la motivación de evasión (alejarse de un aspecto negativo, impulsada por el miedo). Ambos tienen un papel que desempeñar; sin embargo, como señala el psicólogo Andrew Elliot (Universidad de Rochester), "La motivación de evasión está diseñada para facilitar la supervivencia, mientras que la motivación de acercamiento está diseñada para facilitar la prosperidad".

En este documento, lo invitamos a unirse para avanzar de la supervivencia a la prosperidad, aprovechando la oportunidad para trabajar hacia un objetivo realmente positivo: lograr una reputación potente y magnética reforzada por un confiado enfoque de seguridad de ciberorgullo.

Comencemos con un hecho muy básico e indiscutible: los incidentes pueden dañar (y lo hacen) las reputaciones de las empresas. Es muy sencillo: los clientes esperan que mantenga sus datos seguros y sus operaciones en ejecución y, si no puede llevarlo a cabo, encontrarán a alguien que pueda realizarlo. Es más, el riesgo del daño en cuanto a la reputación por los incidentes cibernéticos va en aumento.

El valor de la reputación no es un aspecto nuevo: corresponde a uno de los recursos más fundamentales que una empresa puede poseer (y lo mismo ocurre con las personas, ahora que lo pienso). Los clientes no solo compran una solución, un servicio o un producto, sino también una marca, una idea, una promesa o un objeto mejor. A menudo, la confianza es lo que cierra el negocio.

En la era digital, dos fuerzas clave provocaron que la defensa de la reputación fuera más urgente que antes. El primero es el delito cibernético, que deja expuestas a las empresas al ataque de grupos maliciosos remotos y sin identificar, cuyas acciones pueden derribar a una empresa. El segundo es el contexto digital más amplio de redes sociales, noticias instantáneas y sitios de reseñas abiertos, tales como Trustpilot, G2, Feefo y muchos más. Combinadas, estas dos fuerzas significan que no solo se trata de un frente de batalla más grande y difuso que antes, sino también que el desafío de contener cualquier noticia negativa (incluso los rumores) se vuelve incesante, como un juego de golpear al topo.

Únase a nosotros a medida que avanzamos más allá del riesgo para explorar las oportunidades de administración de la reputación y la ciberseguridad

Debemos hablar acerca del riesgo en cuanto a la reputación a partir de incidentes cibernéticos y, en este documento, lo llevaremos a cabo, gracias a hechos realistas y concretos que debe saber si se comprometerá a defender y proteger la preciada (y bien merecida) reputación de la empresa para obtener un futuro rentable.

Sin embargo, también analizaremos la interacción entre la ciberseguridad y la reputación desde un ángulo completamente nuevo, uno que lamentablemente falta en el discurso moderno acerca del tema. Además de proporcionarle conocimientos fundamentales acerca de los riesgos, lo invitaremos a explorar la riqueza de oportunidades que representa el desafío a la reputación, en el contexto de ciberseguridad y muchos más.

Creemos que una posición simplemente defensiva es lamentable y poco ambiciosa: no se hace justicia a la empresa, los clientes, la misión o los valores. En cambio, proponemos un concepto totalmente nuevo: el ciberorgullo. El miedo desempeña un papel muy válido para obligarnos a tomar medidas necesarias, pero deseamos llevarlo mucho más allá de aquella posición defensiva y a un mundo en el que la reputación se valore, se desarrolle, se celebre y ya no se proteja celosamente como una princesa encerrada en una torre.

Conozca las tres vías en cuanto a la reputación

La reputación no se trata de una construcción monolítica. Se desarrolla por las acciones acumuladas de las tres vías principales y se puede destruir de igual manera por el daño a través de cualquiera de aquellas mismas vías. Estas (sin ningún orden en específico) son las siguientes:

1. Noticias sobre productos
2. Branding
3. Security

En este documento, nuestra principal preocupación es la tercera vía en cuanto a la reputación (la seguridad), pero vale la pena decir algunas palabras acerca de las otras dos primero, ya que existe una interacción significativa entre las tres.

Vía número 1 en cuanto a la reputación: el producto

Esto parece muy sencillo: el producto es bueno, los clientes saben que el producto es bueno y, por lo tanto, lo eligen a usted en vez de los competidores. En un mundo ideal, la reputación dependería del producto y su calidad. Después de todo, ¿no sería maravilloso si todo lo que tuviéramos que realizar fuera crear un producto hermoso y esperar a que las ventas se desbordaran?

El crédito cuando es adecuado: por qué la convicción es todo
Cuando los clientes le compran, acreditan dinero en la cuenta a cambio de productos o servicios. La palabra "crédito" proviene del latín "credere", que significa creer. Esta convicción (o falta de ella) es lo que impulsa las decisiones de compra en todas partes, desde la persona a la empresa más importante. Los clientes eligen sus productos debido a que creen (acreditan) que puede cumplir de una manera que los competidores no pueden. Esta convicción se encuentra detrás de la transacción financiera, que representa la confianza que los clientes depositan en usted. Esta confianza se obtiene y se fortalece a través de uno de los recursos más extraordinarios que la empresa puede desarrollar: la reputación.

... y no solo son los clientes quienes lo acreditan
No debemos olvidar que los clientes no son el único grupo al que le importa la reputación cuando se trata de crédito, convicción y reputación. La empresa debe acceder al crédito financiero real, y el daño en cuanto a la reputación puede afectar de manera negativa la calificación de crédito, lo que dificulta las inversiones y el crecimiento. Las primas de seguros también se pueden ver afectadas de manera negativa por el daño en cuanto a la reputación, ya que las aseguradoras cobran mayores sumas a las empresas cuyas reputaciones en ciberseguridad se consideran más débiles.

Vía número 2 en cuanto a la reputación: la marca

Una vía muy moderna, la marca tiene un grado de influencia en cuanto a la reputación de la empresa que solo crece a medida que el mundo se vuelve más grande (por el tamaño potencial del mercado) y más pequeño (por el poder de Internet) que nunca. La marca aborda el hecho de que los clientes compran más que solo un producto, compran una idea o incluso un sentimiento (a veces, frívolo) al que aspiran. Si el producto es bueno, aunque la marca es deficiente, puede crear, crear y crear con toda su fuerza, pero los clientes no llegarán.

Vía número 3 en cuanto a la reputación: la seguridad

Por lo general, lo que escuchará acerca de la vía de seguridad en cuanto a la reputación es que la falta de ella tiene el poder de destruir cualquier bien logrado por el producto o la marca de una sola vez con el hacha (virtual) del cibercriminal. Cambiaremos completamente la manera de analizar la ciberseguridad en este documento, pero no podemos evitar el hecho, cada vez más lamentable y verdadero, que el daño a esta vía realmente puede provocar enormes consecuencias a cualquier buen trabajo que se llevó a cabo a través de las otras.

Saquemos lo negativo del camino lo antes posible. La vía de seguridad en cuanto a la reputación alude a tres áreas clave, que acompañamos a continuación con las preguntas clave que se plantean en la mente de los clientes:

- Los datos del cliente: ¿me respeta?
- Suministro (frente a la latencia) continuo y confiable: ¿puedo confiar en que cumplirá a tiempo sin excepción?
- Competencia: ¿sabe siquiera lo que lleva a cabo?

Romper el hielo con algunos hechos realistas y concretos

La reputación no puede ser una idea tardía cuando se trata de estrategias de seguridad de TI (o una estrategia comercial de cualquier tipo, ahora que lo pienso). La reputación es el oro de nuestro Fort Knox, se trata del ancla que hace que nuestros clientes crean en el poder de nuestros productos y servicios que no solo se entregarán, sino que también se brindarán mucho más allá que los de nuestros competidores. El mensaje principal de la reputación es la **confianza.**

Cómo sabemos lo que sabemos: Encuesta de riesgos de seguridad de TI corporativa internacional de Kaspersky

Cada año, durante los últimos nueve años, Kaspersky llevó a cabo una gran encuesta internacional de riesgos de seguridad de TI corporativa para detectar exactamente qué atraviesan las empresas cuando experimentan un incidente de seguridad. La encuesta abarca 23 países e incluye datos de casi 5000 entrevistas con líderes de empresas de toda la variedad. Los datos de este extraordinario estudio informan todo lo que realizamos, lo que garantiza que nuestros productos y servicios sigan resolviendo cada problema real para un mundo muy real.

La vía de seguridad en cuanto a la reputación y los resultados: hechos de nuestra encuesta

Es muy fácil dejarse llevar cuando se habla acerca del valor de la reputación y flotar en las nubes de la relajada conversación de marketing (no se trata de que el marketing no tenga un papel que desempeñar), pero el resultado es lo que cuenta. Por ello, nuestra encuesta identifica el costo financiero exacto de los incidentes de seguridad: debemos conocer el tamaño del obstáculo que enfrentamos si deseamos superarlo.

Para los fines de este documento, analizaremos cuatro categorías que confirman las pérdidas financieras específicas relacionadas con la reputación que suceden en caso de un incidente cibernético:

1. Pérdida de ingresos
2. Daño en la calificación de crédito y aumentos en las primas de seguros
3. Costos de RR. PP. para la limitación de daños y la reparación de la reputación
4. Costos de indemnización (el acto de pedir disculpas a modo de compensación financiera)

A continuación, se presenta cómo cada una de estas cuatro áreas se ve afectada por el incidente cibernético promedio para las pymes y las empresas:

Categoría de pérdidas	Pymes del año 2019	Empresas del año 2019
Pérdida de ingresos	USD 13 000	USD 163 000
Calificación de crédito o primas de seguros	USD 13 000	USD 179 000
Costos de RR. PP.	USD 12 000	USD 161 000
Indemnización	USD 5000	USD 72 000
Pérdida TOTAL en cuanto a la reputación	USD 43 000	USD 575 000
Pérdida TOTAL por incidente cibernético	USD 108 000	USD 1,4 millones
% de pérdida debido a la reputación	40 %	41%

El impacto de las pérdidas financieras debido a problemas relacionados con RR. PP.
Además de determinar el alcance de las pérdidas financieras en caso de un incidente cibernético, queremos saber el impacto que tuvieron dichas pérdidas en las empresas. Preguntamos a los encuestados si su organización experimentó algún problema relacionado con RR. PP. (escándalos, crisis públicas) con respecto a incidentes de seguridad en general y filtraciones de datos en particular, durante los últimos 12 meses, y si podrían estimar cuán significativas fueron las pérdidas para su empresa.

De los que experimentaron algún tipo de incidente de seguridad, un gran 77 % afirmó que las pérdidas financieras relacionadas con RR. PP. fueron significativas o muy significativas, mientras que de aquellos que experimentaron una filtración de datos, un 80 % indicó que las pérdidas fueron significativas o muy significativas. Esos porcentajes fueron los mismos para las pymes y las empresas.

No sorprende que las empresas de seguros comiencen a ofrecer soporte de RR PP. como parte de sus paquetes de servicios para corregir los siguientes incidentes cibernéticos. Hiscox (Reino Unido) lo incluye en su cobertura:

Costos de las relaciones públicas:
Los costos razonables que se implementan en nuestro contrato previo por escrito:

1. **para un asesor de relaciones públicas o administración de crisis a fin de ayudarlo a restablecer la reputación de la empresa y responder a los informes de los medios de comunicación, incluido el desarrollo y la comunicación de una estrategia con el fin de reparar la reputación;**
2. **para emitir declaraciones a través de correo electrónico, su sitio web o cuentas de redes sociales, incluida la administración y la supervisión de los sitios de redes sociales; y**
3. **para cualquier otra medida razonable y proporcional que se adopte a fin de proteger o restablecer la reputación de la empresa.**

Lo que realmente conmociona acerca de estas cifras es el hecho de que un 40 % de todas las pérdidas financieras que sufre una empresa tras un incidente cibernético se reduce al daño en cuanto a la reputación. Como referencia, el 60 % restante se pierde por la necesidad de emplear profesionales externos, salarios adicionales del personal interno, sanciones y multas, mejoras de software e infraestructura, capacitación y contratación de personal nuevo.

Si aisláramos el daño en cuanto a la reputación como indicador de pérdidas, podríamos indicar ingenuamente que, tras asegurar su reputación, una empresa podría reducir las pérdidas en caso de un incidente cibernético en un gran 40 %. Evidentemente, este enfoque no tiene ningún sentido práctico (debido a que la reputación de una ciberseguridad sólida solo se puede generar con hechos, no fanfarronería), pero se trata de una manera útil de dar al daño en cuanto a la reputación el lugar que le corresponde como área de preocupación que exige una atención seria y urgente.

Un enfoque integral que se basa en la realidad y enfrenta el futuro con confianza

Sabemos que las tres vías en cuanto a la reputación están estrechamente conectadas y que ninguna se puede abordar de manera aislada de las otras. Estas son buenas noticias: una fuente de inmenso poder que las empresas pueden aprovechar para aumentar su reputación y sus resultados, con la seguridad de que la inversión en una vía genera beneficios en las otras dos. Sin embargo, requiere que nos alejemos de la manera de pensar atomizada y negativa acerca de la ciberseguridad como una "simple" táctica defensiva o que solo yace en el ámbito de TI.

La ciberseguridad puede ser un problema relativamente nuevo, pero el área más amplia acerca de **cómo las empresas abordan el riesgo para su beneficio** es muchísimo más antigua. Para perfeccionar nuestro enfoque de la ciberseguridad no tenemos que reinventar la rueda. Para probar nuestro punto, analizaremos otra industria que enfrentó sus peores riesgos y resultó victoriosa, resistente y lucrativa.

Lo que la industria automotriz tiene que enseñar a las empresas acerca de la ciberseguridad y la reputación

En 1869, la científica irlandesa Mary Ward se convirtió en la primera persona que murió en un accidente automovilístico. Poco más de 150 años después, los accidentes automovilísticos son ahora la novena causa de muerte más común, con 1,2 millones de personas que mueren a nivel mundial cada año. Es increíble retroceder y considerar aquellos riesgos en el contexto de aproximadamente 1400 millones de automóviles que existen en el mundo ahora mismo, con más de 74 millones vendidos cada año.

Los riesgos a los que se enfrentan los fabricantes de automóviles y sus clientes son mucho mayores que los que conllevan los incidentes cibernéticos: hablamos acerca de muertes y lesiones graves, lo que hace que una vulneración de datos parezca insignificante. Desde dicha perspectiva, debería sorprendernos que los fabricantes de automóviles ahora conducen sus campañas publicitarias y de RR. PP. con la seguridad como una característica clave. Imagine ahora a su propia empresa y los riesgos que enfrenta cuando se trata de incidentes cibernéticos: ¿estaría dispuesto a liderar con seguridad? Demasiadas empresas prefieren rezar para que sus clientes ignoren los riesgos de ciberseguridad cuando toman decisiones de compra, rezan también para que no ocurra ningún incidente y, si sucede, lo resolverán lo mejor posible.

Por supuesto, la industria automotriz no siempre fue tan audaz. Durante décadas en que los riesgos (o las muertes, por no decirlo de otra forma) aumentaron de manera exponencial, los fabricantes de automóviles prefirieron deslumbrar a sus clientes con el brillo de otros valores y características: glamour, libertad, diversión, lujo y potencia del motor. Las empresas automotrices solo llevaron la seguridad al centro de atención en los años 80 y presentaron sus tecnologías de defensa proactiva como parte integral no solo de sus productos, sino también de las plataformas de su marca.

Muchas empresas modernas también están atrapadas en una actitud impulsada por el miedo hacia la ciberseguridad y la administración en cuanto a la reputación, que hace eco del retraso de la industria automotriz en considerar la seguridad como factor principal de ventas. Este miedo, que se complica por la incertidumbre en medio de un panorama de riesgos cibernéticos que cambia con rapidez, puede hacer que las empresas pierdan oportunidades de crecimiento increíblemente potentes.

Tome el caso de Volvo, por ejemplo, considerado ampliamente y clasificado de manera independiente como uno de los fabricantes de automóviles más seguros del mundo durante varias décadas. Si me perdona el juego de palabras, esta reputación segura no fue un accidente: Volvo fue una de las primeras empresas automotrices en comprender la relación positiva y rentable entre la seguridad y la reputación, tras liderar y diferenciarse con una audaz campaña publicitaria que cuenta con maniquíes de pruebas de choques. Vale la pena ver el anuncio publicitario para el Volvo 340 del año 1987: 43 elegantes segundos que sirven como una lección perfecta de por qué las empresas deben impulsar sus credenciales de seguridad (el director de ciberseguridad entre ellos) al centro de atención.

El año pasado, la campaña publicitaria de New Gig de Toyota realizó un seguimiento del papel del maniquí de pruebas de choques en la promoción de la seguridad como producto principal y característica de la marca. Esta vez, el maniquí de pruebas de choques está conmocionado al encontrarse sin su puesto de trabajo, gracias a las características de seguridad automatizadas de Toyota que evitan que sucedan accidentes en primer lugar.

Las afirmaciones de seguridad de Volvo se basan en la tecnología de seguridad sólida y, por ello, impulsan su crecimiento

La reputación de la seguridad de Volvo no se disparó a través de una sencilla campaña publicitaria. La campaña solo funcionó debido a que sus afirmaciones eran verdaderas y las clasificaciones de seguridad independientes los respaldaron, una y otra vez, desde entonces. De hecho, en el año 2017, el Volvo XC90 fue denominado osadamente como "El automóvil más seguro del mundo" por los evaluadores independientes más altos posibles, el Instituto de Seguros para la Seguridad en las Carreteras (IIHS).

La ciberseguridad no es diferente de la seguridad para automóviles cuando se trata de garantizar que no son solo palabras, sino también acciones. Esto es verdadero desde dos ángulos. Primero, saber que la empresa es segura le brinda la confianza que necesita para promover realmente la seguridad como valor clave, que se respalda con acciones. Segundo, y quizás lo más evidente, los clientes saben si su proveedor realmente actúa (o solo habla), ya sea por un incidente cibernético que afecta un servicio o filtra datos, o debido a que se vuelven más y más expertos en detectar farsas en los valores empresariales, gritar tonterías y exigir pruebas de acciones significativas.

Antes de que empecemos a contarle cómo Kaspersky puede brindarle confianza para promover el compromiso de seguridad de la empresa de una manera que impulsará el crecimiento e inspirará la confianza de los clientes, creemos que es justo presentar algunas evidencias claras propias, de modo que sepa que actuamos. Hacer afirmaciones acerca de la eficiencia es fácil de lograr; sin embargo, a menos que aquellas afirmaciones se respalden con pruebas independientes (tales como las de IIHS y el Volvo XC90), son irrelevantes.

Estamos orgullosos de afirmar con confianza el hecho de que somos el proveedor de ciberseguridad más probado y premiado del mundo, gracias a un rendimiento constante en varias pruebas independientes que brinda una evaluación mucho más significativa que una sola victoria.

En aquel registro líder en el mundo de rendimiento constante, se encuentran algunos galardones clave recientes que estamos especialmente orgullosos de presentarle hoy mismo:

- La iniciativa de transparencia global de Kaspersky fue probada recientemente por el Paris Call for Trust and Security in Cyberspace (vea el lado izquierdo)
- AV-Comparatives felicitó recientemente a Kaspersky por recibir su premio Producto Mejor Calificado, así como otros premios por pruebas individuales en el 2019
- La Anti Targeted Attack Platform de Kaspersky fue la única solución que demostró una tasa de detección en un 100 % y ningún falso positivo en la prueba de defensa avanzada contra amenazas que ejecutó ICSA Labs en el tercer trimestre del año 2019.
- Este año, Kaspersky logró la certificación ISO/IEC 27001:2013; el estándar internacional que destaca las prácticas recomendadas para los sistemas de administración de seguridad de la información

Estas son solo algunas de las credenciales que nos brindan la confianza para presentarnos ante los 400 millones de usuarios y 270 000 clientes empresariales y decir lo siguiente: **"Lo protegemos, está a salvo".**

Nos gustaría que compartiera parte de aquella confianza, de modo que la voz de la empresa pueda elevarse sobre la multitud y hablar audazmente acerca del respeto que otorga a los datos de los clientes y la capacidad de cumplir a tiempo, sin excepción. A veces, especialmente en el contexto de la crisis de personal en ciberseguridad o cuando los presupuestos y el tiempo se encuentran bajo presión, puede ser difícil representar realmente aquella confianza (o ciberorgullo) de manera que sea atractiva en la base de clientes.

Por ello, diseñamos Kaspersky Endpoint Security Cloud para ofrecer una protección excepcional y preparada para el futuro que no podría ser más fácil de administrar. Surge con tecnologías de protección de última generación y estamos emocionados de contarle acerca de ellas, pero primero debemos profundizar todavía más en lo que vemos como una de las mayores oportunidades perdidas en la historia de los negocios.

El presidente Emmanuel Macron emitió el Paris Call for Trust and Security in Cyberspace en el año 2018 durante el Foro para la Gobernanza de Internet celebrado en la UNESCO y el Paris Peace Forum. El llamado invita a todos los participantes del ciberespacio a trabajar en conjunto e incentivar a los Estados a cooperar con los socios del sector privado, y establece al Centro de transparencia global de Kaspersky como respuesta modelo al Principio 6 (seguridad del ciclo de vida).

"Kaspersky implementa un enfoque único para una mayor transparencia y confianza comprobable en ciberseguridad:
La iniciativa de transparencia global de Kaspersky (GTI) pone en práctica un conjunto de medidas claras de verificación y minimización de riesgos para aumentar la confianza de los usuarios y garantizar que las soluciones de ciberseguridad cumplan y superen los estándares de seguridad y protección de datos empresariales".

¿Por qué las empresas no lideran con sus credenciales de ciberseguridad y privacidad? ¿Por qué no sienten ciberorgullo?

De acuerdo con Forrester, un 32 % de los adultos británicos en línea, un 35 % de los anuncios estadounidenses y alemanes en línea y un 38 % de los adultos franceses en línea no confían en ninguna empresa para que mantenga su información personal a salvo. Además, sabemos que esta confianza (o falta de ella) es un factor clave en las decisiones de compra, que se reduce al crédito. Si se tiene esto en cuenta, es difícil comprender por qué las empresas de todo el mundo pierden la oportunidad de colocar sus preocupaciones de privacidad y ciberseguridad a la vanguardia de lo que comunican a sus clientes.

Avisos de privacidad y la prisión poco ambiciosa de la letra pequeña

Existen joyas preciosas confinadas en la prisión de la letra pequeña a la que se accede por un vínculo de <Aviso de privacidad> que se ubica de manera inadvertida en la parte inferior de las páginas web de empresas de todo tipo. Estas joyas se deben extraer, pulir y colocar en exhibición.

El aviso de privacidad de una empresa promedio cuenta con una breve declaración inicial descriptiva que trata de preocupaciones muy válidas de los clientes acerca del uso de información personal, pero inmediatamente se expande a un larguísimo texto incoherente de jerga legal: poco atractiva e intercalada solo con la muy puntual garantía explícita del valor que la empresa otorga a los datos y la seguridad de sus clientes.

No sugerimos que cada página web o fragmento de material de marketing debería conducir a declaraciones acerca de la ciberseguridad y la confidencialidad de los datos, sino más bien estas deben avanzar de la sombría prisión de la letra pequeña. La ciberseguridad y la confidencialidad de los datos se deben incorporar en toda la empresa de manera integral, una que reconozca la prioridad de dichas preocupaciones como una oportunidad para impulsar el crecimiento de la empresa, en vez de una concesión poco ambiciosa a los requisitos regulatorios.

La regulación no debe ser la única guía de las políticas de ciberseguridad y privacidad

Muchas empresas aceptan la ilusión de que las regulaciones son suficientes como guía para tomar decisiones de ciberseguridad y privacidad. Esto se trata, nuevamente, de las decisiones impulsadas por el miedo y la búsqueda de indemnizaciones, en vez del desarrollo de la excelencia ética y el crecimiento de la empresa.

Primero, las regulaciones se esfuerzan por seguir el ritmo de los avances tecnológicos, ya sea por el lado de la empresa o de los cibercriminales y sus métodos en constante evolución para provocar estragos maliciosos. Si bien es evidente que se deben cumplir las regulaciones, los verdaderos líderes empresariales siempre observarán más allá de las estipulaciones actuales, guiados por la realidad de las innovaciones tecnológicas por un lado y los eternos principios éticos inmutables que (deberían) impulsar las regulaciones en primer lugar.

Las buenas noticias son que, si las empresas aceptan y defienden la centralización de la ética en la ciberseguridad y la privacidad, tal como los analistas de Forrester lo han hecho, se encuentran naturalmente con una potente oportunidad para promover el valor ético de su marca de manera que se respalde con acciones sólidas. Este es un ejemplo concreto de la interacción entre las vías de marca y seguridad en cuanto a la reputación.

Después de todo, una cosa es decir “Tratamos los datos con el máximo respeto y esta es la manera en que cumplimos con todas las regulaciones pertinentes”, y otra muy distinta es retroceder y crear un enfoque ético e integral para que la ciberseguridad y la privacidad se conviertan en características clave del producto y la marca. Cuando las decisiones en ciberseguridad y privacidad se rigen por valores éticos profundamente arraigados y no por regulaciones, los mensajes públicos de una empresa acerca del respeto dejan atrás la sumisión simbólica con las regulaciones y, en cambio, se hace realidad en las percepciones de los clientes actuales y los potenciales.

En resumen, si desea aprovechar la ciberseguridad y la privacidad para impulsar el crecimiento de la empresa, no solo afirma que le importa: lo demuestra, audazmente, en cada oportunidad (pertinente). Es el aire que respira, son los productos que crea, es la cultura de la organización en su conjunto y todos tienen un papel que desempeñar. La organización que logre este objetivo muy posible (como Volvo lo hizo con la seguridad automotriz) asegura un potente y duradero factor diferenciador del resto de la multitud, que permanece paralizada por su hiperenfoque en la regulación a expensas de acciones éticas positivas.

Aproveche la excelente oportunidad perdida hoy mismo y utilice la reputación para impulsar el crecimiento con Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security Cloud elimina los riesgos, lo que brinda a la empresa la confianza para aprovechar la ciberseguridad a fin de impulsar el crecimiento hacia un futuro seguro, rentable y emocionante. Además de saber que la empresa está protegida por el **proveedor de ciberseguridad más probado y premiado** del mundo, podrá compartir esa confianza en todo lo que comunica a los clientes y las partes interesadas. Dicha confianza se traduce en un claro factor diferenciador de los competidores que se quedan atrás en el aprovechamiento de la vía de seguridad en cuanto a la reputación, tales como los fabricantes de automóviles antes de la jugada audaz y lucrativa de Volvo en los años 80.

Kaspersky Endpoint Security Cloud está personalizado para la era de la nube, el trabajo remoto y BYOD, es una solución real y fácil de utilizar que brinda protección y controles potentes a las empresas cuyos objetivos se establecen absolutamente en el crecimiento.

Una de las tecnologías que obtendrá y que nos emociona especialmente es el NUEVO Cloud Discovery, que evita de manera automática que los empleados se tienten con el uso de servicios no autorizados en la nube. Elimina por completo el estrés que puede conllevar tener que microadministrar la creciente gama de servicios en la nube que podrían amenazar potencialmente la seguridad de la empresa.

Además, obtendrá Kaspersky Security for Microsoft Office 365 como parte del paquete: nuestra solución dedicada de defensa para todo el conjunto de Office es fundamental, especialmente debido a que los productos de Microsoft siguen siendo el blanco principal de los cibercriminales.
Ahora que el trabajo remoto se vuelve algo cada vez más común, agregamos dos licencias móviles gratuitas por usuario, de modo que obtendrá una defensa cibernética sólida que reconoce que emplea a personas y no dispositivos. Incluso puede hacer cumplir las políticas de seguridad de manera remota, de modo que se protegerá a los empleados dondequiera que se encuentren, ya sea en una cafetería o en la playa.

Kaspersky Endpoint Security Cloud se aloja en la nube, de modo que no necesita hardware o software, ni debe pagar por aprovisionamiento ni mantenimiento. Obtendrá una protección instantánea con políticas de seguridad predefinidas desarrolladas por nuestros profesionales y se incluye en una suscripción mensual para liberar recursos financieros.

Para nuestros 4000 expertos internacionales, **la seguridad realmente es todo.** Vivimos, respiramos y amamos la ciberseguridad con el fin de que las empresas de todo el mundo puedan tomar nuestra pasión y los galardones que esto supone para crear una base sólida que les permita avanzar, explorar y descubrir el futuro.

Converse con nosotros acerca de cómo puede sentir ciberorgullo y crear una reputación segura para impulsar el crecimiento con **Kaspersky Endpoint Security Cloud**.

Noticias de amenazas cibernéticas: www.securelist.com
Noticias de la seguridad de TI: latam.kaspersky.com/enterprise-security

latam.kaspersky.com

kaspersky BRING ON THE FUTURE

2020 AO KASPERSKY LAB. TODOS LOS DERECHOS RESERVADOS. LAS MARCAS REGISTRADAS Y LAS MARCAS DE SERVICIO PERTENECEN A SUS RESPECTIVOS PROPIETARIOS.