Los ciberriesgos impactan en las organizaciones en áreas que no siempre se tienen en cuenta

- "Solving the Cyber Puzzle: The Unexpected Ways Cyber Risk Impacts Your Business": Nuevo informe de Aon sobre las principales tendencias 2020 en Ciberseguridad

- Identificadas seis áreas de riesgo infravaloradas: propiedad intelectual, fusiones y adquisiciones, jubilación, directivos, delitos informáticos y las propias compañías

4 de marzo de 2020 **-** Aon plc (NYSE:AON), empresa líder en servicios profesionales globales que ofrece un amplio abanico de soluciones de riesgos, capital humano y salud, ha presentado el informe "Solving the Cyber Puzzle: The Unexpected Ways Cyber Risk Impacts Your Business". En esta edición 2020, el informe anual sobre predicciones de ciberseguridad de la firma alerta a las empresas de que los ciberriesgos pueden originarse desde cualquier canal digital, incluso desde aquéllos más inesperados.

El informe identifica seis áreas de riesgo que a menudo no están valoradas suficientemente y a las que las organizaciones deben prestar atención. Éstas son propiedad intelectual, fusiones y adquisiciones, jubilación, C-Suite o equipo directivo, delitos informáticos y, por último, la propia responsabilidad corporativa de la compañía.

6 Riesgos: Principales conclusiones

- El robo, la apropiación indebida o las infracciones contra la **propiedad intelectual**, esto es, activos no tangibles como las patentes, marcas, copyrights, dominios o secretos comerciales, suponen cada vez más un riesgo para las organizaciones. Entre 2005 y 2018, el valor de los activos intangibles pertenecientes a las cinco mayores empresas por capitalización de mercado se ha incrementado de 9,28 a 25,03 trillones americanos de dólares, y este tipo de activos constituye el 80% del valor de las empresas del S&P 500. La propiedad intelectual es clave para la innovación y crecimiento del negocio, y siendo cada vez más un objetivo de los delincuentes informáticos, el peligro acecha. Un paso fundamental es la correcta identificación de estos activos críticos o "joyas de la corona" que deben ser protegidos.

- La **adquisición, desinversión o fusión** con otra empresa puede suponer que la adquiriente o nueva empresa herede tanto futuras pérdidas ocultas derivadas de riesgos ciber como vulnerabilidades. Lo alarmante es que menos del 10% de estas transacciones incluyen una due diligence específica en ciberseguridad y ciberriesgos. Ejecutar un acuerdo de este tipo sin conocer la situación en tema ciber de la otra compañía puede poner en riesgo el capital invertido y el retorno futuro de la operación, e incluso la reputación de la marca o su valor.

- Las organizaciones tienen habitualmente una falsa confianza en la seguridad de los planes de **jubilación**. Los fondos y planes de pensiones manejan gran información sensible de partícipes y beneficiarios, dando además entrada a importantes sumas de dinero. Cada vez más el acceso a los mismos se realiza a través de plataformas digitales y dispositivos móviles susceptibles de ser hackeados. ¿Cómo se protege la información, y cuál es el grado de concienciación de estas entidades frente al cibercrimen? El objetivo final de todas las acciones debe ser proteger los datos de accesos no autorizados.

- Los **directivos** (C-Suite) de las empresas son 9 veces más propensos a ser víctimas de un ciberataque, ya sea mediante técnicas de ingeniería social o cuentas de correo comprometidas. Estos perfiles son perseguidos por diversos motivos: influencia, valor reputacional o acceso a datos de interés, pero sin duda detrás de todo ello está el propósito claro de obtener un beneficio económico fraudulento. Por ello, necesitan ser asegurados dentro y fuera del entorno digital y físico de la organización.

- Los **delitos informáticos** son ya uno de los mayores riesgos para las organizaciones. Se estima que el ransomware alcanzará pérdidas por 20.000 millones de dólares en 2021. El robo, el fraude y la explotación a través de internet fueron responsables de más de 2.700 millones de dólares en pérdidas financieras en 2018. Para las empresas que trabajan con proveedores y terceros, el compromiso del correo electrónico comercial es un riesgo crítico.

- A nivel **corporativo**, las sociedades cotizadas tienen obligaciones de comunicación de incidentes de ciberseguridad. De forma similar, los altos directivos son los responsables últimos de marcar la estrategia y proteger a la empresa frente a los ciberriesgos y cibercrimen. Las múltiples consecuencias de la materialización de las ciber amenazas (demandas colectivas, sanciones, costes relacionados y lucro cesante, entre otros) pueden tener un impacto de gravedad en el balance y continuidad de la empresa.

Este informe viene a complementar y ampliar el panorama de las amenazas en ciberseguridad que ya eran conocidas y que reflejábamos en nuestro reciente informe de C-Suite Series, en colaboración con Financial Times, "Prepare for the expected. Safeguarding value in the era of cyber risk".

Acerca de Aon
Aon plc (NYSE: AON) es una empresa líder en servicios profesionales globales que ofrece un amplio abanico de soluciones de riesgos, capital humano y salud. Nuestros 50.000 empleados en 120 países desarrollan al máximo las posibilidades de nuestros clientes utilizando data & analytics propios que nos permiten ayudar a reducir la volatilidad y mejorar los resultados. Para conocer más visite http://www.aon.com/spain/ o nuestra plataforma de contenidos NOA.

Sigue a Aon España en las redes sociales:
www.twitter.com/Aon_Espana / www.facebook.com/aon.espana1 / https://www.linkedin.com/company/aon-spain

Contacto:
Aon /Dirección de Comunicación
91 340 51 41 / 629 66 50 63
dcomunic@aon.es

Empower Results®