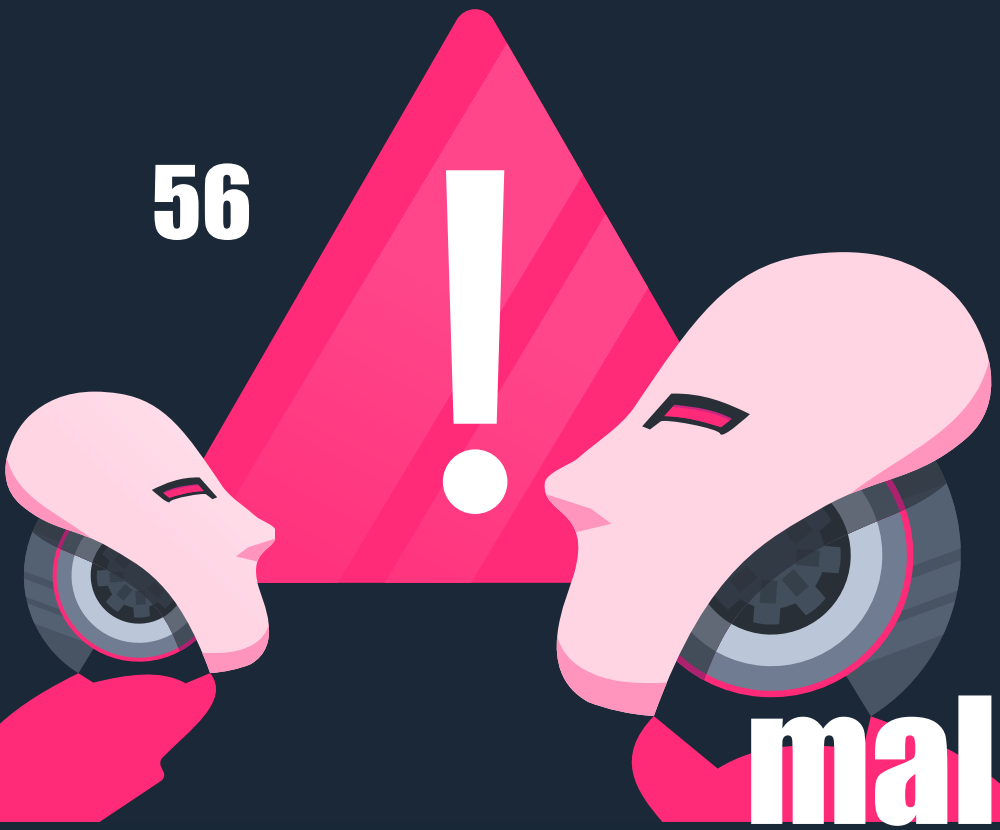

IA maliciosa, nuevo ciberriesgo reputacional

La ciberdelincuencia es cada vez más habitual y especializada. Desafortunadamente, la pregunta que se deben hacer las empresas hoy no es si van a sufrir un ciberataque en algún momento, algo que prácticamente se da por sentado, sino cómo de eficientes y rápidas van a ser su respuesta y su recuperación una vez que suceda. Por ello, entender en detalle cómo funcionan las pólizas de ciberriesgos y los procesos de reclamaciones es fundamental para limitar el impacto financiero y operativo de los ataques.

Las pólizas de ciberseguridad son una herramienta de protección del balance y la cuenta de resultados frente al impacto económico que se deriva de un ciberataque o de un fallo de sistema. Las principales razones por las que cada vez más empresas deciden apoyarse en uno de estos seguros son, entre otras, la dependencia creciente de la tecnología para la producción o la prestación de servicios; el aumento en la frecuencia y la gravedad de los ciberataques y las brechas en la seguridad de los datos; el almacenamiento de un volumen cada vez mayor de datos personales; y posibles daños reputacionales.
Este último área, el de la preocupación por el impacto en la reputación a largo plazo que pueda sufrir la marca tras un ciberataque o un robo de datos crece. Y ahora se suma un nuevo protagonista al contexto: el uso malicioso de la inteligencia artificial (IA), una tecnología que, si bien se ha convertido en una herramienta de impulso de la eficiencia, la innovación y la toma de decisiones, representa un riesgo reputacional significativo para las compañías y sus directivos, con efecto directo en su línea de negocio, si es utilizada de forma malintencionada por parte de terceros.

Uno de nuestros estudios recientes, denominado 2023 Global Directors' and Officers' Liability Survey Report, y realizado en colaboración con Clyde & Co LLP en 40 países, arroja que la preocupación a nivel global de los directivos y gestores ante los riesgos relacionados con la IA

Ulysses Grundey
Director de D&O y Riesgo Reputacional de FINEX en WTW

y el machine learning (aprendizaje automático) crece un 42%. El robo de datos sensibles, el espionaje corporativo, la difusión de información falsa, la suplantación de identidad, la manipulación de fotografías, vídeos y voz, entre otros, son algunos de los riesgos que más preocupan a los directivos y gestores de riesgos en España, en un baremo de 51%, el mismo nivel de preocupación que les suscita el Covid-19 y la posibilidad de nuevas medidas de bloqueo.

En este contexto, la gestión del riesgo reputacional en relación con la IA es de vital importancia para las organizaciones. Una buena gestión de este riesgo es fundamental para asegurar el éxito a largo plazo de una empresa. Para mitigar estos nuevos ciberriesgos es esencial tomar medidas proactivas y establecer los controles adecuados. Para ello, es necesario contar de antemano con una estrategia cuidadosamente planificada que incluya la identificación previa de los posibles riesgos, su prevención y, en el caso de que ya se haya producido el daño reputacional, contar con las herramientas y los recursos necesarios para mitigarlo. Acciones que, lógicamente, deberían ir acompañadas de una legislación sólida que contribuya a garantizar un uso ético y responsable de la IA desde las administraciones públicas.

Luchar contra este tipo de riesgo reputacional implica, en primer lugar, la correcta y personalizada evaluación de los riesgos, trabajando en colaboración con empresas para identificar áreas de riesgo y evaluar los riesgos específicos relacionados con la IA. Llevar a cabo programas de formación y concienciación sobre los riesgos de la IA dentro de las empresas es también una medida interesante a tener en cuenta.

No menos importante es contar con planes de gestión de crisis específicos para situaciones relacionadas con la IA maliciosa. Saber cómo comunicar de manera efectiva en caso de un problema reputacional es clave. Igual que es muy importante colaborar con expertos en IA que puedan ayudar a evaluar los riesgos y proporcionar asesoramiento en la toma de decisiones éticas. No olvidemos que la propia inteligencia artificial puede ser utilizada tanto para perpetrar daños reputacionales como para mitigarlos.

Auditorías y evaluaciones regulares, investigación y análisis de tendencias, y contar con pólizas de seguros de reputación son áreas también a considerar.

Podemos concluir de todo lo expuesto que la IA ofrece notables beneficios para las empresas, pero también conlleva riesgos reputacionales que no deben pasarse por alto, muchos de ellos ligados a la suplantación de identidad o la manipulación de fotografías, vídeos y voz que vienen a sumarse a otras ciberprácticas delictivas que ya vienen de lejos, como el robo de datos sensibles, el espionaje corporativo o la difusión de información falsa a través de canales digitales.

Controlar estos riesgos requiere un enfoque proactivo en la ética, la transparencia y la responsabilidad. Al adoptar medidas sólidas, las empresas pueden proteger su reputación en esta nueva era de la IA y mantener la confianza de sus stakeholders en un entorno cada vez más digital y propenso a ciberataques. En este contexto, colaborar con expertos para identificar y evaluar los riesgos, llevar a cabo programas de formación y concienciación a la plantilla, saber comunicar de forma efectiva en caso de sufrir un problema reputacional y contar con planes de gestión crisis para situaciones relacionadas con la IA maliciosa dejan de ser opciones para convertirse en imperativos.