Reidertsvo, el enemigo silencioso de las empresas

José Riba Vidal
Socio director
de Riba-Vidal Abogados

Últimamente, los medios de comunicación nos despiertan con escándalos que afectan a compañías, poniendo en duda su reputación y la corrección de sus prácticas ya sean contables, financieras o de gestión.

El resultado en algunos casos será probablemente la deriva hacia una situación concursal, con liquidación de la empresa en el peor de los escenarios, o la toma de control de la empresa por parte de un tercero.

En casos menos críticos el problema se limitará a un perjuicio económico temporal si la empresa es capaz de defenderse al descubrir que está siendo realmente víctima de un ataque o *Reiderstvo*. terminología importada de la antigua Unión Soviética. Esta práctica en los últimos años se ha ido extendiendo paulatinamente al resto del mundo.

Entendemos el *Reiderstvo*, *Raiding* en terminología anglosajona, como la toma de control o el intento de tomar el control de una empresa al margen de la voluntad de sus propietarios o accionistas.

La globalización y la era cibernética ha facilitado estos ataques o tomas de control, permitiendo a los *Raiders* ocultar de forma más efectiva sus prácticas maliciosas y dificultando la defensa legal de las victimas por la complejidad probatoria de los métodos y sus autores, así como por los complejos tramites de extraterritorialidad jurisdiccional que comportan la mayoría de estas actuaciones.

El *Raider,* normalmente a través de un equipo contratado expresamente para la operación, diseñará cuidadosamente su estrategia mediante el seguimiento y análisis de la compañía objetivo durante largo tiempo, detectará sus debilidades y las potenciará o creará en función de sus objetivos. El ataque empezará en el momento en que se considere que se dispone de material suficiente como para obtener buenos resultados y se desplegará en el tiempo, siguiendo una estrategia minuciosamente planificada.

El *Raider*, utilizará su información para determinar el grado de dificultad al que se enfrenta, y ello le llevará a definir tres posibles escenarios de *raiding*:

***a) Raiding* nivel 1**:

El Atacante utilizará mecanismos en total consonancia con la normativa del país en que se realice el ataque, es decir, será absolutamente legal, este será el caso de determinadas OPAS hostiles. Este tipo de *Raiding* en mayor o menor medida siempre ha existido en el mundo empresarial competitivo.

La ilegalidad puede ser subyacente, pues probablemente habrá utilizado mecanismos ilegítimos para la obtención previa de información de la compañía, pero no necesariamente.

***b) Raiding* nivel 2**:

El atacante realizará acciones que podemos considerar “alegales”, no entran en colisión directa con una norma jurídica, bien porque esta no existe (laguna legal), bien porque estas acciones se mueven simplemente en el campo de la moral o de ética.

En algunos casos se utilizarán mecanismos de *lawfare*, entre ellos el hostigamiento de la compañía objetivo, con multiplicidad de requerimientos, denuncias, demandas, querellas; procedimientos judiciales carentes de fundamento con el único objetivo de desgastar la reputación de la empresa al tiempo que sus recursos económicos, sin olvidar las campañas de desprestigio en redes sociales

***c) Raiding* nivel 3:**

El atacante, si los mecanismos anteriores no han funcionado o no lo han hecho de la manera que esperaba, o nunca se planteó opciones sutiles dentro de su estrategia, pondrá en marcha medios claramente ilegales. Utilizará una estrategia global con ataques informáticos, ciberdelitos, o cualquier otro tipo delictivo (amenazas, coacciones, daños materiales etc.) que pueden alcanzar no sólo a la estructura interna de la empresa, sino también a accionistas, directivos, empleados, proveedores, clientes, etc.

En definitiva, estamos ante un fenómeno en crecimiento que puede afectar al tejido empresarial de un país debido a la falta de concienciación de un gran número de empresarios, que en muchos casos sufren las consecuencias del ataque sin saber qué es lo que realmente está pasando. El empresario puede llegar a perder su empresa pensando que han sido un cúmulo de circunstancias desafortunadas las que le han llevado al desastre. El objetivo de los *raiders* pueden ser tanto las grandes compañías como las pymes.

Estos ataques pueden generar, no lo descartemos, problemas de geopolítica en función de que el ataque pueda tener cobertura desde algún Estado y el objetivo sean infraestructuras críticas de otro país.

La protección de las compañías pasa necesariamente por la concienciación de las mismas, de la existencia y dimensión del problema y la utilización de protocolos “*antiraiding*” operados por equipos de seguridad corporativa y abogados, especializados en tecnología y métodos de inteligencia ■