Ciberseguridad, la gestión de un riesgo ineludible

Por ***Inés Leopoldo***, ex directora en YPF

A medida que las empresas incrementan sus interconexiones, crecen los riesgos cibernéticos; sin embargo, no todas están preparadas para prevenirlos.

La digitalización de los procesos operativos de la industria del petróleo y del gas permiten nuevas oportunidades para mejorar la productividad y reducir los costos. Simultáneamente, han desaparecido, en gran medida, los límites tradicionales entre los sistemas de información corporativos (IT) y los sistemas de control industrial (ICS/OT), sistemas informáticos utilizados para gestionar las operaciones industriales en oposición a las operaciones administrativas (IT). En la industria del petróleo y del gas, los sistemas de control industrial son aquellos que se utilizan para monitorear y controlar las operaciones en toda su cadena de valor.

A medida que esta interconexión avanza, les implica a las empresas una nueva gama de riesgos cibernéticos. Sin embargo, la mayoría no ha mantenido el ritmo de avance en términos de preparación ante estos riesgos.

La brecha cibernética, intencional o no, tiene consecuencias que pueden ser graves: desde comprometer la información confidencial hasta desencadenar una falla o caída del sistema con la consecuente disminución de los ingresos, los daños a la reputación, los incidentes ambientales, las sanciones legales y, en casos extremos, riesgos de la integridad física de las personas.

En 2017 ocurrieron algunas de las ciberamenazas más notables de la historia, que afectó a millones de consumidores y miles de empresas, como Equifax y Uber. En particular, el 12 de mayo comenzó una infección masiva de equipos a nivel mundial, tanto de personas como de organizaciones, donde la causa fue un *malware* del tipo *ransomware* que bloqueaba el acceso a los archivos de la computadora afectada y solicitaba un rescate para permitir el acceso.

Ese hecho fue un punto de inflexión en la sensibilidad sobre la definición de ciberseguridad y el riesgo. El ataque *ransomware WannaCry* afectó a más de 200.000 sistemas en 150 países. Aunque no fue diseñado para dirigirse a los sistemas de control industrial, *ransomware WannaCry* logró infiltrarse en las redes de ICS y, en algunos casos, significó la inactividad de los procesos industriales.

Entre las empresas afectadas podemos mencionar al fabricante de automóviles rumano Dacia propiedad de Renault de Francia, que llevó a Renault a detener temporalmente la producción en varios sitios para evitar la propagación del ataque. Asimismo, el fabricante mundial de automóviles Nissan, también informó que su planta de fabricación del Reino Unido había sido afectada.

Otras amenazas pueden ser mucho más sofisticadas, como ataques planificados y dirigidos, diseñados específicamente para acceder a redes industriales. Un ejemplo es *Crash Override,* el *malware* utilizado para piratear una estación de transmisión de electricidad en Ucrania en 2016, además de otro *malware* que apuntaba a sistemas de seguridad en instalaciones petroquímicas en Medio Oriente, y que reflejan vectores de ataque emergentes claramente focalizados en las infraestructuras críticas.

El ritmo de las infracciones cibernéticas no disminuye, al contrario, está en aumento. En parte, lo estamos haciendo demasiado fácil para los atacantes. ¿Cómo? Los empleados caen en sofisticados esquemas de *phishing* o suplantación de identidad (intento de obtener información confidencial de forma fraudulenta, como el nombre de usuario, una contraseña o detalles de tarjeta de crédito, por ejemplo), olvidan instalar actualizaciones de seguridad

o usan contraseñas débiles. Sumado a que cada día trabajamos más en dispositivos móviles que no están debidamente protegidos. Por su parte, las empresas no invierten lo suficiente en ciberseguridad o aplican soluciones parciales o transitorias a sus sistemas cuando se descubren problemas.

Kaspersky Lab, en conjunto con la consultora Bussiness Advantage, en 2017 realizó un estudio de investigación global entre profesionales de ICS/OT con el fin de comprender sus percepciones e identificar los problemas más importantes que afectan a sus organizaciones.

De manera reiterada, los expertos en ciberseguridad insisten en que los entornos industriales no están protegidos lo suficiente, debido a que las empresas subestiman el impacto de los riesgos cibernéticos y solo invierten en medidas de seguridad después de algún ataque. Así es que más de la mitad (un 54%) de las organizaciones muestreadas han experimentado al menos un incidente en su sistema de control industrial en los últimos doce meses, con poco más de uno en cinco (un 21%) experimentando dos incidentes en el mismo período de tiempo.

La mayoría de los incidentes (el 53%) fueron causados por *malware* y virus convencionales. Los segundos en incidencia, más de un tercio (el 36%) de las empresa, fueron los dirigidos. Si bien la tercera razón más importante para todos los incidentes fue el error humano (un 29%), se calificó como la sexta de mayor preocupación, lo que indica una brecha en las percepciones. Asimismo, tres de cada cuatro empresas (un 74%) esperan un ataque a su sistema de control industrial.

Los datos muestran que el número de personas objetivo en los ataques es alto y destaca que dentro de las organizaciones no se debe subestimar la amenaza de la seguridad interna, por ejemplo, una persona que inserta una memoria USB en una PC industrial e infecta los sistemas de control.

Las amenazas cibernéticas se encuentran entre las principales preocupaciones de los directores ejecutivos, de acuerdo con la reciente Vigésima Primera Encuesta Global de Directores Generales (CEOs) de PwC. A nivel global es una de las preocupaciones que más creció junto con el terrorismo (4to y 2do lugar, respectivamente). Aunque las percepciones varían significativamente en las diferentes regiones, para los directivos de Norteamérica, las ciberamenazas están primeras en sus preocupaciones, mientras que en Latinoamérica, el populismo lidera la tabla, y las ciberamenazas ni siquiera se encuentran entre las primeras diez.

Es curioso que a pesar de lo generalizadas que son las amenazas y de la importancia que representa para los Estados Unidos, el 44% de los 9.500 ejecutivos consultados en la Encuesta Global sobre Seguridad los Sistemas de la Información de PwC en 2018 dice no tener una estrategia general al respecto. Eso da una idea del trabajo que queda todavía por hacer dentro de las empresas. Muchos directores no confían en que la gerencia maneje las amenazas cibernéticas. Asimismo, se confirma una vez más que los incidentes atribuidos a piratas informáticos, competidores y otros intrusos han disminuido. Sin embargo, los que se atribuyen a personas con información privilegiada, como terceros, incluidos los proveedores, los consultores los contratistas y los empleados, se han mantenido más o menos iguales (cercano al 30%).

En particular, en la industria del gas y del petróleo estas amenazas se ven reflejadas en la apropiación indebida de información sensible como datos de pozos y reservas, accesos no autorizados y manipulación de sistemas de "pipelines" o bien en el robo de datos de inventario de crudo o productos refinados, entre otros incidentes.

Deloitte en su informe "Securing Industrial Operations in Oil & Gas" de 2017 indica que al realizar evaluaciones de madurez ante ciberamenazas para una amplia gama de empresas de energía han observados que el índice de madurez de la industria de petróleo y gas en su conjunto es de 2,2 en una escala de 5, mientras que la posición recomendada es de 3,7. Claramente, hay mucho trabajo por delante y es esencial que se tomen medidas para identificar los riesgos en entornos ICS, con políticas rigurosas, procedimientos establecidos y protocolos de emergencia que administren esos riesgos para que la empresa esté en la mejor posición, en orden de asegurar la continuidad de sus operaciones, aun ante el inevitable evento de ataque. Y sobre todo entender que la ciberseguridad no es solo responsabilidad exclusiva de un sector especializado de la compañía, como puede ser Sistemas o Seguridad de la Información, es un trabajo en equipo de todas las áreas operativas de la misma y debe ocupar un lugar destacado en la agenda de la alta Dirección, fundamentalmente a través de la integración en la gestión de riesgos de la organización y en las políticas aplicables. Por ello, cada vez más ciertos entes reguladores, en especial los que rigen las compañías que cotizan en los mercados de capitales, como la SEC, empezarán a exigir mayores precisiones en cuanto las acciones preventivas, los controles o políticas específicas de cada compañía en cuanto a ciberseguridad.

Hace dos años el Word Energy Council nos advertía que "Al igual que otras industrias, la industria del petróleo y el gas ha estado trabajando para mejorar la ciberseguridad, que es o debería ser una preocupación prioritaria en los directorios y en la alta Dirección. Las compañías de energía deben ver al ciberriesgo como un riesgo propio del negocio… Deben trabajar para concientizar a todas las partes interesadas (empleados, accionistas, proveedores) sobre el impacto de los ciberataques…" (*World Energy Perspective,* 2016).