VERTICE SEGUROS

Nuevos riesgos asechan el transporte

CAPÍTULO 09

LOS HACKERS ATACAN EL TRANSPORTE

Por José Antonio Ricaurte R.
Luisa Ricaurte Espinosa

El siguiente documento está basado en hechos reales que suceden permanentemente en el mundo del transporte, y por lo tanto reflejan situaciones de las operaciones logísticas. Sin embargo, todos fueron alterados en algunas de sus partes para proteger a quienes estuvieron involucrados o salieron perjudicados.

Estas narraciones fueron escritas únicamente para servir como documento de trabajo en procesos educativos, en la implementación de programas de administración de riesgos y seguros de transporte. De ninguna manera para juzgar a los protagonistas o a una industria o empresa en particular.

Ninguno de los casos pretende culpar o señalar a alguien, y los únicos nombres exactos que se conservaron fueron aquellos que fueron hechos públicos, que la comunidad conoce por diferentes medios.

Si usted identifica una situación presentada con alguna que le haya sucedido, será simple coincidencia.

CAPÍTULO 09

LOS HACKERS ATACAN EL TRANSPORTE

Los riesgos cibernéticos ya llegaron al transporte. Atacaron a la naviera más grande del mundo, una empresa de más de 700 buques, y a varias que están entre el grupo de las cinco más importantes a nivel global, además de emblemáticos puertos europeos y empresas de transporte terrestre. Entonces ¿qué es todo esto? El costo de la modernidad que llega con muchos beneficios, pero también con nuevos riesgos. El transporte no es ajeno a esto y ya lo está sufriendo.

Mientras escribíamos este libro, la línea naviera CMA-CGM era víctima de un fuerte ataque cibernético que mantuvo su *website* fuera de funcionamiento por varios días. Casi todas las semanas nos enteramos de ataques similares a la infraestructura del transporte, que en este caso afortunadamente se resolvió en menos de una semana y aparentemente sin consecuencias graves. Sin embargo, durante el fin de semana anterior un exportador de bienes a Estados Unidos contrató una empresa de transporte en México para que transportara unos contenedores. Al llegar al puerto encontró que alguien ya lo había hecho a su nombre. ¿A quién robaron? ¿Al puerto, al exportador o al transportador?

Puede ser que fuera a todos; este evento sucede cada vez con más frecuencia porque los sistemas son muy vulnerables y aparentemente fáciles de hackear. Sin embargo, para los gerentes de logística los ciberataques son un riesgo lejano y todavía no lo tienen contemplado en su mapa de riesgos. Nosotros les estamos recomendando que lo incluyan, pues estos siniestros son cada vez más frecuentes y lo seguirán siendo.

La naviera A.P. Møller-Mærsk, una de las empresas más importantes del mundo marítimo (tal vez la mayor), fue víctima de un ciberataque el 27 de junio de 2018, principalmente en el área de transporte de contenedores. La naviera danesa fue una de las principales afectadas por la variante del virus informático "Petya" que atacó de forma masiva a

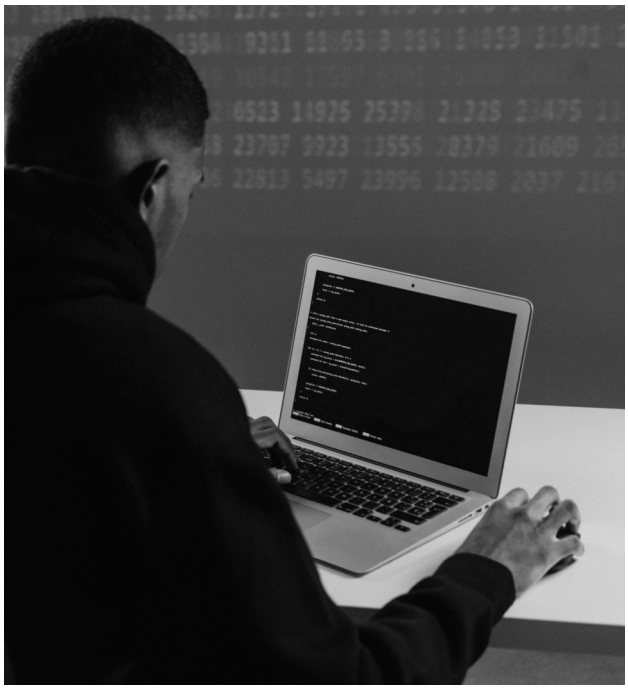
decenas de grandes empresas e instituciones europeas, principalmente en Ucrania y Rusia y que fue distribuida a través de un programa de contabilidad ucraniano. La empresa estimó que los daños causados por el ciberataque mundial le costaron 255 000 000 de euros. Puede ser el siniestro más grande por un ciberataque (sin los bancos) en el mundo.

En Colombia a los ejecutivos de la naviera les tocó recurrir a sus computadores personales y empezar a recibir las reservas de los barcos en tablas de Excel por más de un mes, tal cual como suena. Sin embargo, aunque el ataque afectó a muchas áreas de la compañía, no hubo ni pérdida ni filtración de información a terceros.

Ahora bien, la naviera danesa no ha sido la única, la francesa Saint-Gobain y la farmacéutica estadounidense Merck también tuvieron filtraciones en sus sistemas.

El virus informático "Petya" es similar a "WannaCry" que en mayo del 2020 perjudicó a más de 200 000 usuarios en 150 países, entre ellos al sistema de sanidad británico (NHS). En septiembre del 2019 un ataque de *ransomware* afectó al puerto de San Diego en Estados Unidos. Varios archivos y servicios de acceso público fueron encriptados, impidiendo el acceso a su información. Los atacantes solicitaban una suma importante de dinero en *bitcoins* para desbloquear el acceso a los archivos, lo que obligó a detener algunos servicios para evitar la propagación del *ransomware*.

Otro caso sucedió en julio de 2019. COSCO (una de las grandes líneas navieras más del mundo y una compañía del gobierno chino) fue víctima de un ataque *ransomware* que afectó la conexión de sus oficinas en Long Beach, perjudicando la comunicación con clientes, buques, terminales y proveedores. Las líneas telefónicas y el servicio de correo electrónico presentaron fallos, obligando a la compañía a apagar las conexiones de las demás regiones donde operaban para evitar una propagación.



Por otra parte, en septiembre del 2018 el puerto de Barcelona fue blanco de un ataque. Sin embargo, por la obligación que exige ser muy prudente con la información comercial, el puerto no dio mayores detalles acerca de la intrusión. Lo cierto es que varios de sus servidores fueron impactados por el ciberataque, lo que obligó a lanzar un plan de contingencia diseñado específicamente para este tipo de incidentes.

En su momento, el puerto anunció que el ciberataque no afectaba a la parte marítima, pero la entrega y recepción de mercancías sí podía sufrir ciertos retrasos, que *se tratarán de minimizar con el plan de contingencia activado*, según el comunicado de la Autoridad Portuaria de Barcelona. Los gerentes de logística saben que esto se traduce en multas y sanciones de las líneas navieras al no devolver el contenedor a tiempo. Un retraso de esta naturaleza en un puerto colombiano puede significar una multa de 100 USD diarios por contenedor, que es lo que usualmente se acuerda en los contratos de comodato.

Igualmente, el puerto belga de Antwerp fue víctima de un ciberataque en el 2011. Aparentemente, un grupo de narcotraficantes logró acceder al sistema que controlaba el movimiento y posición de los contenedores. El sistema les brindaba información a los criminales acerca de la ubicación y los detalles de seguridad de los contenedores. De esta manera, conseguían robar mercancía y contenedores enteros antes de que sus verdaderos dueños los solicitaran.

Pero los ataques no son exclusivos de los terminales portuarios, los buques también lo han sido y tal vez, con peores consecuencias. La Cámara Marítima Internacional (ICS por sus siglas en inglés), la principal asociación comercial internacional para la industria naviera, en su documento "Directrices sobre seguridad cibernética en buques[1]" menciona varios casos. Dentro de los más importantes se encuentra el ataque con virus al ECDIS de un buque que fue diseñado para navegar sin papeles y, por lo tanto, no llevaba cartas de navegación físicas. Estos ciberataques demuestran que la seguridad cibernética no es un tema alejado de la realidad, ni mucho menos de la industria marítima y portuaria. Debe ser asumida con total responsabilidad y prioridad para mitigar las vulnerabilidades seguramente ya existentes en los sistemas de información.

1. CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL BIMCO, *The Guidelines on Cyber Security Onboard Ship*, 2018, https://iumi.com/uploads/2018-Cyber_Security_Guidelines.pdf.

Es por ello que los puertos y buques que transportan mercancías son consideradas —junto con las centrales nucleares y algunas redes viarias— como las nuevas infraestructuras críticas en ciberseguridad. Los daños potenciales que podría causar un ciberataque a gran escala en el sector marítimo son tremendos.

Ciberataques en Colombia

La información de ciberataques a empresas de transporte en Colombia es muy difícil de conseguir. Sin embargo, conocemos algunos incidentes. El puerto de Buenaventura que hoy en día administra carga en varios terminales ha sido tradicionalmente víctima de todo tipo de extorsiones durante muchos años y las primeras víctimas son los transportadores que han tenido que pagar sus "peajes" para poder entregar los contenedores sin incidentes. Hemos visto que estas amenazas se han trasladado a otras modalidades.

Las empresas de transporte que trabajan en esa zona también han sido víctimas de ciberataques en sus propios sistemas. Sin embargo, se guarda silencio al respecto porque de alguna manera se convierte en un mal antecedente que se puede convertir en un problema comercial al afectar su reputación.

Nosotros hemos tenido información de dos de ellos sucedidos entre el 2018 y el 2019. Una reconocida empresa de tecnología contrató a una empresa de transporte para que transportara dos contenedores desde una de las terminales de Buenaventura. El transportista asignó los camiones y cuando los envió a recoger los contenedores la respuesta del puerto fue: "ustedes ya los recogieron".

En estos terminales los administradores les asignan contraseñas a los transportadores registrados para que ellos puedan verificar qué contenedores deben recoger y cuándo. Alguien violó la seguridad del sistema, remplazó las contraseñas y recogió la mercancía en nombre del transportador. Se perdieron dos contenedores de 40", cada uno con 450 000 USD en mercancías.

Nuestra primera reacción fue concluir que el transportador tenía un problema de seguridad interna, pero había muchos indicios de que eso no era posible: les había sucedido a funcionarios de total confianza quienes contaban con muchos años de experiencia en la empresa. Incluso se sometieron voluntariamente a la prueba del polígrafo, saliendo negativa.

Evidentemente, no era una situación de infidelidad de uno de sus empleados, por lo que tenía que ser una falla en los procedimientos de registro. Antes de que se tuviera claridad sobre lo que había pasado, sucedió otro caso similar, en esta ocasión con unos contenedores que contenían celulares de ultima generación. Evidentemente, lo que estaban vulnerando eran los sistemas del puerto.

Después de un periodo de un año se conocieron tres casos similares, lo que despertó aún más sospechas sobre una violación a la seguridad del sistema del puerto para tener acceso a información privilegiada y robar los contenedores. Unas personas habían estado hackeando el sistema del puerto durante varios meses y no se habían percatado. Lo mismo le sucedió a una de las más grandes universidades de Latinoamérica cuyo sistema estuvo vulnerado por más de dos años.

A muchos nos inquieta la seguridad del transporte en Colombia, entre ellos, los puertos del Caribe y del Pacífico, pero también las empresas de transporte. Cuando empezamos a estudiar estos sucesos, nos hemos encontrado varios casos de secuestro de la información. ¿Cuántas extorsiones se estarán pagando en Buenaventura como consecuencia de esta nueva modalidad? De lo que sí estamos seguros es que hay más de una y probablemente varias en desarrollo.

El cyber siniestro

Una de las dificultades de analizar el riesgo cibernético es que no se tiene claridad cómo un evento de ataque se puede convertir en una pérdida patrimonial y, sobre todo, quién resultará afectado. Sin embargo, hay muchos ejemplos de las consecuencias de un ataque en la infraestructura del transporte. Siempre se debe hablar de los perjuicios que se puedan demostrar, en cabeza de los dueños de la carga o responsables de su custodia. Estos pueden ser algunos ejemplos de perjuicios económicos:

- Pérdida de las mercancías, por desaparición, robo o simplemente por no saber dónde están.
- Multas o sanciones por autoridades aduaneras.
- Multas o sanciones por demoras en el retorno del contenedor a la línea naviera (pueden ser de hasta 120 USD por día por contenedor).
- Costos extras por bodegajes en puertos o aeropuertos.
- Gastos en fletes por llevar a la mercancía a su destino original, cuando un ciberataque cambia el destino.
- Aprensión de mercancías por parte de la aduana al incumplir un procedimiento.
- Pérdidas de itinerarios o reservas en buques.
- Carga perecedera dañada por demoras.
- Reembarques por envíos equivocados.
- Maniobras de cargue y descargue innecesarias..
- Lucro cesante por demoras o pérdidas.

ASPECTOS JURÍDICOS

Ante los recientes y cada vez más frecuentes ciberataques, surge la pregunta de si el transportador debe responder en el evento en que la mercancía sufra de alguna pérdida o daño, o si se genera algún perjuicio por un retraso. Esto, teniendo presente que ni en la regulación nacional como internacional se prevé expresamente un ciberataque como una causal de exoneración en el transporte marítimo.

Si bien la exoneración de responsabilidad del transportador marítimo varía según la legislación aplicable (ley nacional, Reglas de la Haya, Reglas de la Haya-Visby, Reglas de Hamburgo o Reglas de Rotterdam), se puede afirmar que, de forma general, para que el ciberataque proceda como causal de exoneración deberá acreditarse que el siniestro no fue causado por culpa del transportador, sus agentes o empleados, y que los mismos tomaron todas las medidas que razonablemente se podían exigir para evitar el hecho y sus consecuencias. En este sentido, el ciberataque debe ser un hecho irresistible e impredecible que de forma alguna sea imputable al deudor.

Lo anterior trae importantes implicaciones para la gestión de riesgos del transportador, pues este no puede desconocer los nuevos peligros que trae consigo los avances tecnológicos y, en consecuencia, debe implementar las medidas de prevención que correspondan para evitar estos sucesos y poder mitigar sus consecuencias.

Tomado de: CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL BIMCO, *The Guidelines on Cyber Security Onboard Ship*, 2018, https://iumi.com/uploads/2018-Cyber_Security_Guidelines.pdf.

Ahora bien, las anteriores consideraciones también son relevantes para los demás intermediarios en el transporte de mercancías como, por ejemplo, el agente de carga y el comisionista de transporte.

Por un lado, en Colombia el comisionista de transporte adquiere los mismos derechos y obligaciones del transportador[2] y, en consecuencia, la gestión de riesgos de ciberataques es igualmente relevante para los comisionistas de transporte, pues estos deberán responder como el transportador ante el remitente o destinatario de las mercancías. Lo mismo sucederá en el evento que un agente de carga sea eventualmente considerado como un comisionista de transporte.

Por otro lado, existen importantes consideraciones en el evento que quien sea víctima de un ciberataque sea el agente de carga y no el transportador. Si bien en dicho escenario no estaríamos ante un evento de pérdida de la mercancía, pues por definición el agente no tiene control sobre la operación de transporte, sí podría suceder que, por ejemplo, en virtud del referido ataque el agente pierda el registro sobre la ubicación de la mercancía y, en consecuencia, se incurran en costos adicionales por demoras en la recogida de la carga. Así pues, ¿quién será el responsable en estos escenarios?

El agente de carga es una figura que no está regulada en la ley colombiana, pero su función tradicional ha sido la de actuar como un intermediario entre el remitente de la carga y el transportador en la celebración del contrato de transporte, para lo cual actúa como mandatario del remitente y no del transportador[3]. En este sentido, sus obligaciones serán aquellas propias de la ejecución de dicha obligación (la coordinación de las labores del transporte de las mercancías) y las relativas al mandato comercial representativo[4], junto con las que se establezcan contractualmente, pudiéndose exonerar únicamente bajo los supuestos contemplados en el referido contrato, probando la debida diligencia y cuidado o por fuerza mayor[5].

Lo anterior implica que, del mismo modo que el transportador, los agentes de carga también deberán implementar mecanismos para prevenir y mitigar los ciberataques, so pena de ser considerados responsables civilmente por los daños que dicha falta de cuidado conlleve. Esto, teniendo especial consideración que los ciberataques ya no son eventos aislados y ocasionales, sino circunstancias que cada vez más hacen parte del día a día en el transporte de mercancías, en un mundo que se

2. Artículo 1313 del Código de Comercio.

3. José Vicente Guzmán Escobar, Contratos de transporte (Bogotá: Universidad Externado de Colombia, 2009).

4. Corte Suprema de Justicia, Sala de Casación Civil, Sentencia del 5 de febrero de 2009. Exp. 2001-00142-01.

5. Artículo 64 del Código Civil.

encuentra en una acelerada digitalización y transformación digital de sus modelos de negocio.

CONSEJOS PARA EL MANEJO DE LOS RIESGOS

Los riesgos de ciberseguridad representan un riesgo para los proveedores, más que para los dueños de la mercancía. Así pues, realmente el inconveniente se causa en los sistemas de puertos, aeropuertos, líneas navieras, aerolíneas, operadores de puertos o aeropuertos y transportadores terrestres.

¿Cómo se puede tener control sobre este complejo mundo logístico? Los dueños de la mercancía pueden verse seriamente perjudicados si no tienen control del movimiento de sus contenedores y, realmente, el riesgo no está en sus manos, salvo la correcta selección de sus proveedores. Sin embargo, siempre existirá la posibilidad de mitigar el riesgo de un ciberataque a sus proveedores, mediante el manejo de la información de los movimientos de forma paralela.

TIPS PARA EL PROGRAMA DE SEGUROS

El riesgo cibernético se asegura mediante una póliza diferente a la del transporte de mercancías. Las coberturas de esta póliza son las siguientes:

1. Pérdidas causadas a terceros

- **Responsabilidad por privacidad:** se pagarán los daños y los gastos por reclamaciones de privacidad.

- **Responsabilidad por seguridad de la red:** se pagarán los daños y los gastos por reclamaciones de seguridad de la red.

- **Responsabilidad por contenidos electrónicos:** se pagarán los daños y los gastos por reclamaciones de contenidos electrónicos.

- **Ciber extorsión:** se pagarán los daños y los gastos por ciber extorsión pagados por el asegurado actuando en alguna de las circunstancias de justificación previstas en el artículo 32 del Código Penal.

- **Pérdida de activos digitales:** se pagarán los costos de recuperación en razón a un incidente de activos digitales.

- **Interrupción del negocio:** se pagará la pérdida por interrupción del negocio que surja durante el periodo de indemnización y los costos de recuperación que surjan de un incidente de interrupción del negocio.

2. Exclusiones Generales

No se amparan los daños o gastos por cuenta de cualquier reclamación:

- Directa o indirectamente causada por el asegurado o por cualquier persona por la cual el asegurado sea legalmente responsable.

- En la que se alegue, se base en, surja de o sea atribuida a un daño corporal o daño material.

- Por incumplimiento de cualquier contrato, garantía, acuerdo o promesa.

- En la que se alegue o se base en cualquier tipo de discriminación ilegal; humillación, acoso o conducta indebida que se relacione con discriminación; y prácticas laborales indebidas.

- En la que surja de honorarios, gastos o costos pagados al asegurado.

- En la que se base en cualquier acto culposo, hecho, circunstancia o situación que ha sido objeto de una notificación escrita, así como en cualquier falla, interrupción o corte del servicio de acceso al internet suministrado por un proveedor de servicio de internet.

- En la que se alegue incendio, humo, explosión, rayo, viento, inundación, terremoto, erupción volcánica, ola de marea (tsunami), deslizamiento, granizo, fuerza mayor o cualquier otro evento físico, como quiera que sea causado.

- En la que se alegue guerra, invasión, actos de enemigo extranjero, terrorismo, hostilidades o guerra, huelga, toma, motín, asonada, guerra civil, rebelión, revolución, insurrección, conmoción civil.

- Que surja de cualquier validación, invalidación, infracción, violación o apropiación indebida de cualquier patente o secreto comercial por parte del asegurado.

- En la que se base en una apropiación indebida de cualquier derecho de autor, marca de servicio, nombre comercial, marca de comercio y otra propiedad intelectual de cualquier tercero, así como una recolección de datos no autorizada, subrepticia, o culposa.

Sin embargo, estas coberturas están incluidas en el programa E-CARGO como amparo adicional.

REFERENCIAS

Normatividad internacional

Reglas de la Haya [Convención de Bruselas para la unificación de ciertas reglas en materia de conocimientos de embarque], 25 de agosto de 1924.

Reglas de la Haya-Visby [Protocolo de Bruselas], 23 de febrero de 1968.

Reglas de Hamburgo [Convención de las Naciones Unidas sobre el transporte marítimo de mercancías], 31 de marzo de 1978.

Reglas de Rotterdam [Convenio de las Naciones Unidas sobre el Contrato de Transporte Internacional de Mercancías Total o Parcialmente Marítimo], 11 de diciembre de 2008.

Normatividad nacional

Decreto 410 de 1971. Por el cual se expide el Código de Comercio. 16 de junio de 1971. DO:33339.

Ley 57 de 1887. Sobre adopción de Códigos y unificación de la legislación nacional [Código Civil]. 15 de abril de 1887. DO: 7019

Jurisprudencia nacional

Corte Suprema de Justicia. Sala de Casación Civil. Sentencia del 5 de febrero de 2009. Exp. 2001-00142-01.

Doctrina y otros

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL. *The Guidelines on Cyber Security Onboard Ship, 2018.* https://iumi.com/uploads/2018-Cyber_Security_Guidelines.pdf.

Guzmán Escobar, José Vicente. *Contratos de transporte.* Bogotá: Universidad Externado de Colombia, 2009.

———. "El agente de carga." *Revista E-Mercatoria* 4, no. 1 (junio 26 de 2005). https://revistas.uexternado.edu.co/index.php/emerca/article/view/2103/1880.

———. E*l Contrato de transporte marítimo de mercancías bajo conocimiento de embarque*. Bogotá: Universidad Externado de Colombia, 2007.