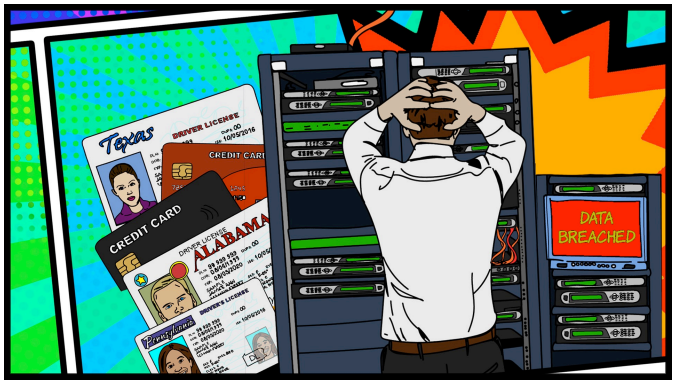
Equifax y su abuso de confianza

Equifax es un de las tres más grandes agencias de calificación de riesgos en los EE. UU. El 7 de septiembre de 2017 la empresa anunció una brecha de la ciberseguridad que expuso la información de más de 143 clientes en los EE. UU., o sea, aproximadamente 44 por ciento de la población de este país. La brecha ocurrió por la vulnerabilidad de la página web se Equifax. Los hackers consiguieron obtener los nombres, fechas de nacimiento, direcciones, número de licencia de conducir, números de seguro social, y algunos números de tarjetas de crédito de los clientes, lo cual puso a muchos en peligro de usurpación de identidad. Los oficiales de Equifax se dieron cuenta del pirateo el 29 de Julio de 2017, más de un mes antes de avisar a los clientes afectados. La empresa advirtió que el acceso desautorizado había ocurrido entre mediados de mayo hasta julio de ese año.

Esta no fue la primera vez que Equifax tuvo que enfrentar el hacking debido a fallos en el sistema de seguridad la de la empresa. Previamente en maro de 2017, Equifax sufrió otra brecha. En esta instancia la empresa notificó a un menor número de clientes bancarios y contrató a una firma de seguridad informática para ayudar con la investigación de la brecha. Aunque esta incidencia no fue públicamente anunciada por Equifax, no habían encontrado evidencia de que los datos fuesen robados ni accedidos por partes desautorizadas. Todavía antes, en diciembre de 2016 un investigador en la seguridad informática examinó los servidores de Equifax y les advirtió que sus sistemas estaban vulnerables al mismo tipo de ataque que ocurrió en 2017. Eventualmente, Equifax llegó a parchear las vulnerabilidades, pero no lo hizo hasta después de la brecha a mediados de 2017. Tras una investigación por un equipo de ciberseguridad independiente después de la brecha del 2017, otros fallos en la seguridad fueron encontrados.

El periodista Stephen Gandel detalló el proceso que Equifax implementa para verificar si los datos se los clientes fueron comprometidos. Después del descubrimiento de la brecha el 29 de julio, no fue hasta dos semanas después que el equipo de 225 expertos en la ciberseguridad de Equifax pudo reportar al Director Ejecutivo que la firma había sido pirateada. Pasaron 2 días más hasta que Equifax pudo declarar incuestionable el hecho de que los datos habían sido comprometidos. 5 días después la Junta Directiva de Equifax fue notificada. Dos semanas más pasaron antes de que el público fuera notificado de la brecha. Gandel escribió que, “es importante entender que lo que pasó en Equifax no fue un simple fallo tecnológico, pero algo más importante, un fallo en la gerencia y gobernación corporativa.”

Poco después de anunciar la brecha en septiembre de 2017, la prensa descubrió que cuatro ejecutivos principales de Equifax habían vendido valores de $1,8 millones en los días después del descubrimiento de la brecha. Equifax llevó a cabo una investigación interna y concluyó que ninguno de los ejecutivos sabía de la brecha en momento que vendieron los valores. Sin embargo, otro ejecutivo, el Director de Informática principal Jun Ying vendió casi $1 millón en valores solo unos días antes de anuncio de la brecha el 7 septiembre. El 8 de



septiembre las acciones de cayeron el 14 por ciento. Ying evitó más de $117.000 en pérdidas que hubiera sostenido si vendiera después de la declaración.

Después de haber anunciado el pirateo, Equifax dirigió a los clientes a una página web donde podrían averiguar si sus datos habían sido comprometidos. Los usuarios tenían que introducir su apellido y los últimos dígitos de su número de seguridad social. También tenían que marcar una casilla de verificación para acordar con las condiciones de uso de Equifax. Estas condiciones incluían una cláusula escondida que enumeraba que el uso de esta página web obligaba al cliente a abandonar sus derechos a levantar una demanda colectiva en contra de Equifax.

En septiembre de 2017 la Oficina de Protección Financiera del Consumidor de los EE. UU. abrió una investigación en la brecha por parte de los consumidores. Un cambio en el liderazgo de la Oficina demoró la investigación, y todavía en abril de 2018 no se ha dado ningún paso en el caso. En marzo de 2018 la Comisión de Bolsa y Valores levantó cargos criminales por uso de información privilegiada contra Ying.

Concepto: la aversión a las pérdidas

Perspicacia ética:

La gente suele tener una aversión a las pérdidas más de que gozan de las ganancias, y asumirán mayores riesgos para evitar una pérdida de los que asumirán para obtener el alza. Este parece resultar particularmente cierto cuando se comete un error. Muchas veces el error es cometido por el mero descuido, pero si el error sale a la luz podría costarle al quien erró la reputación, el trabajo e incluso la libertad. Para evitar sostener tales pérdidas, la gente encubriría sus errores y las consecuencias, a veces con mentiras creadas en el momento.

Cuando Equifax cayó víctima al hacking y sufrió una brecha de sus datos que comprometió la información de casi la mitad de la población de los EE. UU., eso fue grave. Mostró la incompetencia por parte de Equifax. Pero Equifax no llegó a reconocer su error e intencionalmente intentó de esconder la brecha. En vez de notificar al consumidor inmediatamente que su información personal podría haber sido comprometida, los líderes de la empresa demoraron seis semanas en notificar al público. Irónicamente, en vez de evitar los daños a su reputación, el fallo de Equifax de no reconocer sus errores agravó los problemas.

Preguntas de discusión:

1. ¿De qué manera representa el caso de Equifax un ejemplo de la aversión a las pérdidas? Explcia.
2. El periodista Stephen Gandel encontró que varias semanas habían pasado antes de que Equifax notificara al público. ¿Por qué piensas que demoraron tanto? ¿Piensas que la empresa estaba tomando cuidado al analizar la situación, o estaba tratando de encubrir sus errores? Explica.

3. Aunque la brecha a mediados de 2017 fue la brecha de seguridad más grande en la historia de Equifax, no había sido la primera. ¿Por qué crees que la empresa no adoptó medidas más agresivas para reforzar la seguridad de los datos después de las brechas anteriores? Si fueras un ejecutivo en Equifax, ¿qué hubieras hecho al darse cuenta de la brecha?
4. ¿Piensas que fue la aversión a la pérdida que motivó a Jun Ying a entrar en el uso de información privilegiada? ¿Por qué o por qué no?
5. ¿Piensas que una empresa que guarda la información identificable personal de sus clientes está éticamente obligada a informar a los clientes de cada brecha? ¿Por qué o por qué no? ¿Hay algunas instancias en que una empres debería esconder información de sus clientes? Explica tu razonamiento.
6. ¿Puedes pensar en toras empresas que han enfrentado una brecha de datos en que la información personal de los usuarios fuera comprometida? ¿Cómo respondió la empresa? ¿Crees que la empresa demostró la aversión a las pérdidas? ¿Por qué o por qué no?
7. ¿Puedes pensar en otra situación sobre la cual has leído en que una empresa cometió pequeños errores, pero luego intencionalmente los encubrieron? ¿Cómo afecta a la inclinación que tienen las personas a admitir que cometieron un error si tienen que enfrentar la posibilidad de responsabilidad jurídica por indemnización de prejuicios?
8. Dennis Gentilin sugiere que la aversión a las pérdidas es una motivación significativa detrás de los delitos cometidos por líderes porque, por supuesto, tienen más que perder: “Hay una motivación por el comportamiento dentro de las organizaciones que va más allá del dinero y el poder. La gente dentro de la organización, y sobre todo los más poderosos y superiores, han trabajado durante año para lograr el estatus o el título que han llegado a apreciar, es una parte central de su identidad, y define quiénes son. Cuando su posición se ve amenazada, sea por el desempeño débil, sentimiento de incompetencia, cambios en la estructura organizacional, o el riesgo de que se descubriera actividad ilícita, la respuesta natural en todos estos casos es ir al extremo para defender y proteger la posición. Lo que motiva esta reacción defensiva es el temor asociado con la pérdida de su estatus y su título, y las pérdidas financieras y estilo de vida que permite la posición. Por extensión, lo que se juega es justamente todo su ser y su identidad.” ¿Te parece tener razón esto? Discute.
9. ¿Encuentras difícil admitir tus propios errores? ¿Piensas que es difícil para la mayoría de la gente admitir que cometieron errores? Explica.
10. El caso de Equifax demuestra los obstáculos y varios sesgos y comportamientos que incluyen la miopía moral, el sesgo del conformismo, y el pensamiento de grupo. ¿Puedes identificar estos y otros conceptos de la ética del comportamiento en acción en este caso de estudio? Explica y discute su significancia.

Bibliografía:

Una brecha de la ciberseguridad en Equifax dejo vulnerable los datos financieros de casi todos https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/
Mientras que Equifax amasaba cada vez más datos, la seguridad era una de las charlas promocional en su campaña propagandística

https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html
La brecha masiva de datos de Equifax podría afectar a la mitad de la población de los EE. UU.
https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686
El escándalo gigantesco de hacking de Equifax podría costar $70 billones
https://www.vanityfair.com/news/2017/09/equifax-hack-lawsuit
El pirateo de la página web de Equifax expuso los datos de acerca de 143 millones de consumidores estadounidenses
https://arstechnica.com/information-technology/2017/09/equifax-website-hack-exposes-data-for-143-million-us-consumers/
Equifax no es capaz de proteger los datos, pero sí de mantener un secreto
https://www.bloomberg.com/gadfly/articles/2017-10-03/equifax-can-t-protect-data-but-it-can-keep-a-secret
Equifax había sufrido un pirateo casi cinco meses antes de la fecha en que lo anunció
https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed
Equifax había sido advertido
https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning
La falta de parchear un error que quedaba por dos meses condujo a la brecha masiva de Equifax
https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/
Tres gerentes de Equifax vendieron acciones antes de que se revelara el hacking
https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack
El Exejecutivo de Equifax enfrenta cargos de uso de información privilegiada en conexión con la brecha de 2017
https://www.nytimes.com/2018/03/14/business/equifax-executive-insider-trading.html
Un Exejecutivo principal de Equifax es acusado del uso de información privilegiada
https://arstechnica.com/information-technology/2018/03/senior-equifax-executive-charged-with-insider-trading/
Los consumidores han declarado miles de quejas contra Equifax con respecto a la brecha. El gobierno aún no ha hecho nada.
https://www.vox.com/policy-and-politics/2018/4/30/17277172/equifax-data-breach-cfpb-elizabeth-warren-mick-mulvaney
Los orígenes de los fracaso éticos: Una lección para los líderes
https://www.worldcat.org/title/origins-of-ethical-failures-lessons-for-leaders/oclc/971052714