La reputación corporativa frente a las brechas de ciberseguridad

Erick Iriarte Ahon

Introducción

En tiempos digitales la ciberseguridad termina siendo un elemento diferenciador entre aquellas compañias que resguardan la información de sus usuarios/consumidores y la protegen como su propia información de aquellas compañias que simplemente usan la información de sus usuarios sin desarrollar medidas de resguardo de la misma; sin embargo el quiebre de la ciberseguridad, mostrando grietas en el armatoste de una organización, puede implicar que los consumidores y otros stakeholders (en especial shareholders) puedan tomar decisiones que puedan afectar la estabilidad financiera de una empresa, teniendo en cuenta que se puede afectar la reputación corporativa al enfrentar brechas de ciberseguridad y la forma como se enfrentan las mismas.

Problema de Investigación

¿Las brechas de ciberseguridad implican un impacto en la reputación corporativa de las empresas para todos los stakeholders, o solamente para aquellos que puedan tener un poder de decisión directa (shareholders)?

Propósito de la Investigación

Reconocer el impacto en la reputación corporativa el revelado de brechas de ciberseguridad por parte de una compañía y la forma de enfrentar dichas brechas, analizando tanto la perspectiva de los consumidores como de los shareholders.

Significancia de la Investigación

La tecnología digital implica un constante cambio; esto implica fundamentalmente que tan rápido como desarrolla una solución de protección digital hay quienes encuentran brechas en dichos mecanismos de protección digital, es una constante (o debería serlo) la inversión en ciberseguridad para prevenir afectación a la información de usuarios/consumidores, así como de trabajadores internos, así como

información propia de la organización. Si bien el tema esta siendo explorado ya en diversos ambitos geográficos, para América Latina sigue siendo una temática no relevante o inadecuadamente explorada (Lehude, 2019; Lehude, 2020; OEA, 2018, OEA, 2019). Pero se debe entender tambien cual es la reacción de los diversos actores frente a la problemática, en especial consumidores y accionistas (Kamiya et al, 2021).

Un punto de partida.

'It takes 20 years to build a reputation and five minutes to ruin it' (Warren Buffett)

La ciberdelincuencia es una preocupación para los accionistas, ya que la vulnerabilidad a la ciberdelincuencia amenaza la viabilidad de las operaciones comerciales y, por lo tanto, la rentabilidad futura de la empresa. Los inversores pueden rebajar el valor de las acciones de la corporación, provocando que su valoración de mercado disminuya. (Smith et al, 2018). Sin embargo el enfoque que se plantea parte de la premisa que la afectación solo esta en el ambito de los shareholders, y no de todos los actores como plantea Kamiya et al (2021) que ademas es el aspecto que compartimos.

El ciberdelito produce altos rendimientos con bajo riesgo y un costo relativamente bajo para el pirata informático. A diferencia de otros tipos de delitos, el ciberdelito permite a los piratas informáticos esconderse detrás de las pantallas de las computadoras y no tener confrontaciones físicas. (Smith et al, 2019)

Hemos de aclarar ademas que el enfoque de Smith et al va hacia el crimen en si (cibercrimen) y no necesariamente a los instrumentos de prevención del crimen (ciberseguridad), siendo que ello tambien se refleja en diversa literatura en la medida que se presume todo acto de ciberataque como delito, asimismo se debe añadir que dentro del cibercrimen tambien se añaden los delitos de ataques a activos gubernamentales que pueden realizarse a nivel de gobiernos (y aquí entramos más en el ambito de la ciberguerra).

Smith et al (2018) citan a Fama (2018) en relación a la teoría de mercado de capitales eficiente como marco referencial para entender la afectación de las acciones frente a un hecho de un cibercrimen. Dada su relevancia es conveniente tomarlo en consideración como parte del presente artículo.

> This theory states that in an efficient capital market all new, price relevant information is immediately included in asset prices. Thus, assuming that the market is efficient and given that no other event occurred on a certain day, the change in an asset's price as a reaction to a certain event (on that day) can be interpreted as the price effect of that event (Fama, 2018)

Si añadimos lo concluido por Amir et al (2018) que la reacción del mercado a los ataques divulgados es de hecho pequeña, pero la reacción del mercado a los ataques ocultados (y descubiertos posteriormente) es negativa y significativa, tenemos que el escenario es claro sobre el real impacto de como las brechas de seguridad afectan a las compañias.

Ciberseguridad

La ciberseguridad se ha convertido en uno de los asuntos de mayor relevancia para todas las organizaciones, en todos los sectores y en todos los paìses (Corradini, 2020). Es ademas un aspectos critico y protege la información y activos de las compañias (AlGhamdi et al, 2020).

La investigación en ciberseguridad empezó a finales de los 1960 (Eling et al, 2021) y se ha venido desarrollando bajo diferentes nombres incluyendo seguridad informática o computacional y seguridad de la información, y con un auge mas novedoso bajo el concepto de "gestión de ciber-riesgo"

Si aunamos lo expresado por Eling et al (2021) con lo expresado por Smith et al (2018) que el primer cibercrimen ocurrió en 1970 en relación al New York's Dime Savings Bank y siendo que el primer reporte sobre el tema fue publicado en 1973 por el Stanford Resarch Institute (Eling et al, 2021) estaremos que al menos desde hace

casi 50 años tenemos los términos de cibercrimen y ciberseguridad dando vueltas en el ecosistema empresarial.

Pero, ¿a qué nos referimos cuando hablamos de ciberseguridad?. Siguiendo la Resolución 181 de UIT (2010) que referencia a la definición establecida por la Recomendación ITU-T X.1205, se define ciberseguridad como:

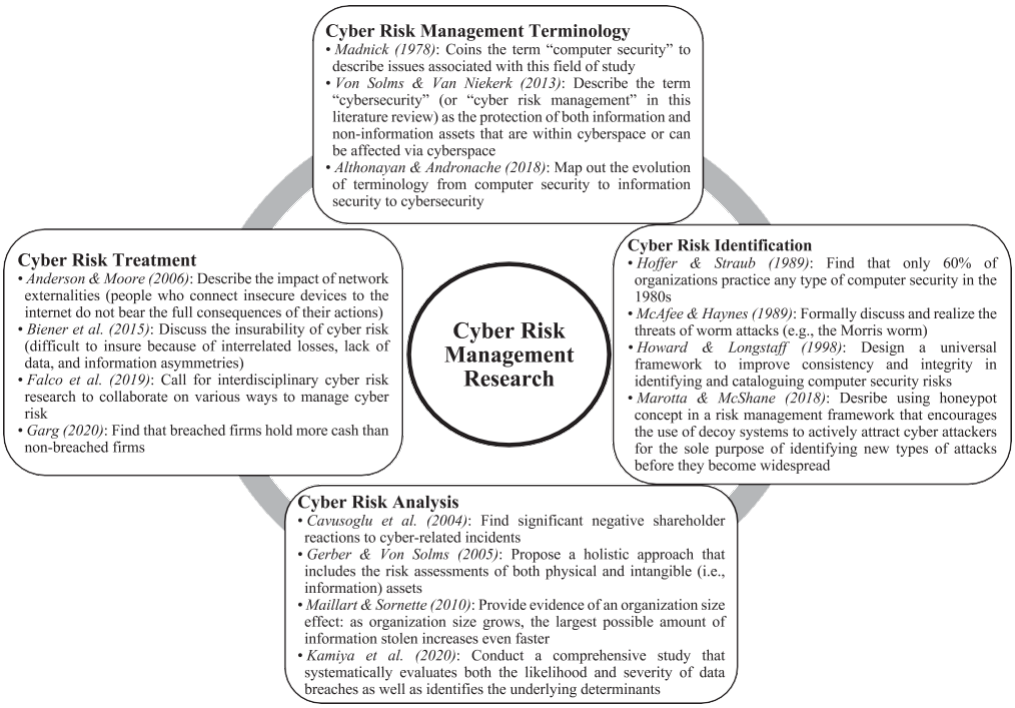
> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:
>
> - Availability
> - Integrity, which may include authenticity and non-repudiation
> - Confidentiality

De otra parte Eling et al (2021) referencian a Von Solms y Van Niekerk para disginguir entre ciberseguridad y seguridad de la información. Siendo que el segundo abarcaria a la protección de la información (sea en entorno digital o no), mientras que el primero iria sobre los activos digitales o no, pero tambien sobre los no activos como pueden ser las personas, dentro de un ecosistema, pudiendo utilizar el ciberespacio para almacenar o acceder a dicha información.

Para clarificar referenciaremos los diagramas de Eling et al (2021) sobre la literatura en la materia de ciberseguridad.

Figura 1

Highlights of cyber risk management research since the 1960s



Nota: Tomado Cyber risk management: History and future research directions, Eling et al (2021)

Del lado de la ciberseguridad, el desarrollo de estandares tuvo un diferente camino al de la protección de datos personales. La BS 7799 (estandar británico para seguridad de la información) desarrollado en 1995, fue el sustento de la ISO 17799-1, que traslado de un estandar local a un estándar internacional los temas de seguridad de la información, esto en el año 2000. Sin embargo la ISO 17799 se transformaría en la ISO 27002 (parte de la gama de las ISO 27000).

CEOs y Alta Dirección de organizaciones de todos los sectores y todos los tamaños consideran cada vez más al ciberataque como uno de los mayores riesgos a los que se enfrentan. Pero, por lo general, sigue existiendo una brecha entre su conocimiento y comprensión del riesgo y la gestión de una estrategia informada de resiliencia cibernética que ayuda a habilitar en lugar de obstaculizar el negocio y sus operaciones. (Lehude, 2020; Wilding, 2016).

Si bien el cumplimiento normativo de normas de ciberseguridad aún es incipiente a nivel de las empresas, dado a la falta de regulación existente en la materia (Lehude, 2020), no significa que de uso ya existente de manera derivada por las medidas de seguridad que se deben adoptar para el resguardo de los datos personales. (European Union, 2016; APEC, 2015).

Romanosky et at (2011) hacen un extenso analisis sobre las brechas de seguridad en relación al robo de identidad (por lo tanto de datos de seguridad social, nombres, y numeros da tarjeta de credito, por ende información financiera) desde los datos de la Federal Trade Comission.

Hay tambien un cuestionamiento por parte del sector privado de ver el cumplimiento en materia de estandares como un sobrecosto, sin embargo la transformación digital, y en concreto la acelerada por el período de la pandemia, ha mostrado que las organizaciones que han desplegado un cumplimiento normativo de dichas legislaciones (ya de por si obligatorias) terminan teniendo ventajas competitivas frente a otras que no lo realizan , siendo además mandatorio en diversas jurisdicciones (Bayoli, 2020), aunque aun sectorialmente por ejemplo las obligaciones para el sector bancario en materia de ciberseguridad ligada a la continuidad del negocio, y por ende, en beneficio de los clientes (OEA, 2018).

Si bien los esfuerzos por tratar de desarrollar un set de herramientas mínimos para los Directorios en materia de ciber-resilencia (WEF, 2017) o manuales para que sepan desde los boards como supervisar los riesgos en materia de ciberseguridad (OEA, 2019), el proceso de transformación digital no ha calado profundamente en la

estructura empresarial, relegando estos temas como técnicos y no como estratégicos o de continuidad de negocios.

Hemos de añadir que la construcción de mínimos se encuentra presente en el desarrollo de estandares (ISO, 2018), de manera tal que se construye estandares que pueden ser deplegados en su formato mínimo pero sobre el cual se pueden construir mas herramientas, para un mayor nivel de seguridad, sin que esto significa que tengan vinculación con un cumplimiento normativo específico, en la mayoría de los casos por la falta de regulación sobre la materia. (Lehude, 2020).

En la actualidad defender la información de una organización es pues uno de los aspectos mas relevantes del manejo y gestión de tecnología, siendo así no siempre un ciberataque logra su cometido de obtener información pero el ataque en si mismo puede dañar la reputación de la compañía. (Smith et al, 2019)

Eling et al (2021) plantean (parafraseando al WEF) que:

> “Fourth Industrial Revolution (4IR) technologies,” such as artificial intelligence (AI), quantum computing, Internet of Things (IoT) devices, 5G networks, cloud technologies, and blockchain have the potential to drastically increase efficiency and boost economic growth, but also to increase cyber risk resulting in losses of up to US$6 trillion in 2021 (Eling et al, 2021)

El Impacto Reputacional

Veh et al (2018) hace una extensa recopilación de información sobre reputación corpoprativa pero se enfoca que los atributos de la organización y la percepción por parte de los stakeholder, esta idea se verá reflejada sobre todo en lo expresado por Kamiya et al (2021).

De los primeros artículos sobre el impacto reputacional y por ende el impacto en el valor en el mercado de las empresas por brechas de seguridad es el artículo de Cavusoglu et al (2004). Se plantea una clasificación de impactos transitorios y permanentes.

> The transitory costs of security breaches include lost business and decreased productivity resulting from the unavailability of the breached resources; la- bor and material costs required to detect, contain, repair, and reconstitute breached resources; costs associated with evidence collection and prosecu- tion of the attacker; costs related to providing information to customers and the public; and other media-related costs.
>
> Permanent, or long-term, costs have more far-reaching effects on the breached firm's future cash flow. These costs are related to the loss of custom- ers who switch to competitors, inability to attract new customers due to per- ceived poor security, loss of trust of customers and business partners, legal liabilities arising from the breach, and the cost of attackers' access to confi- dential or proprietary information. Perceptions of increased business risk may also translate into increased insurance costs for the firm and higher capital costs in debt and equity markets. (Cavusoglu et al, 2004)

He et al (2019) apuntan que la investigación ha desarrollado los aspectos de impacto de corto plazo pero que los de largo plazo no se han logrado medir adecuadamente a contrapartida de lo que expone Cavusoglu et al (2004). He et al (2019) enfocan su análisis en lo que impacta en I+D, consistente con lo expresado por Kamiya et al (2021) sobre la afectación al ecosistema. Mayor posibilidad de vulneración, menor riesgo, menor inversión en innovación, mayor inversión en ciberseguridad, es una idea que aflora entre los textos planteados.

Por su parte Choong et al (2017) plantean la idea de costos directos e indirectos como resultante de las brechas de seguridad, reafirma la idea de afectación en la valorización de la organización desde el lado de los inversores en el corto plazo, y en el largo plazo si no se corrigen los errores afectara de manera permanente a la compañía.

Sin bien ya era conocido el impacto de brechas internas (tal como revela Andoh-Baidoo et al, 2010), la literatura encontrada hasta ya entrada la decada de 2010

no hace mayor referencia al ocultamiento de información, y más bien reafirma un impacto directo sobre los consumidores que puede verse mitigado de acuerdo a literatura posterior.

Andoh-Baidoo et al (2010) plantean previamente (y refutando estudios previos) que no solamente las brechas de seguridad que afectan afectación de información personal son las que generan retornos negativos. Añaden ademas que la aparición de internet afectó los procesos de ciberseguridad dado que hay mayor espacio para la penetracción externa, siendo que previamente la casuística enfrentaba a casos internos. Hemos de discrepar que si bien hay mayor cantidad de casos externos aparentes, la eficacia de brechas de seguridad internas, son mayores.

En contrapartida a Andoh-Baidoo et al (2010), el trabajo de Kamiya et al (2021) vuelve a focalizarse en la afectación de datos personales, en especial los financieros.

De hecho Kamiya et al (2021) expresan en sus hallazgos como es la reacción de los diferentes actores frente a las brechas de seguridad.

> We find that attacks that do not involve the loss of personal financial information do not cause a significant shareholder wealth loss. In contrast, attacks where personal financial information is lost involve a significant shareholder wealth loss. (…)
>
> Thus, although it is possible that we underestimate out-of-pocket costs, most of the shareholder wealth loss is attributable to other factors, such as the new information about the likelihood and the costs of cyberattacks for the target, and the impact of this new information on the risks borne by stakeholders. (…)
>
> In the absence of new information from a cyberattack, the firm's risk management policies and risk appetite should stay the same. In contrast, we find that attacked firms invest more in risk management and decrease their risk appetite by reducing risk-taking incentives of management.

> Last, if the impact of an attack reveals only idiosyncratic information about the target, we would expect industry competitors to benefit from the attack. In contrast, we find that shareholders of these competitors experience a shareholder wealth loss as well. Such a result is consistent with the view that the new information revealed by the attack increases the expected costs of attacks for competitors as well. (Kamiya et al, 2021)

En palabras de Kamiya et al (2021), el impacto puede no ser tanto si hay personas informadas que los sistemas de información pueden ser vulnerables, más si la Alta Gerencia invierte en ciberseguridad, pero aún así pudiera tener efecto sobre los accionistas (y por ende sobre las acciones), más cuando la información que se pudiera haber obtenido tiene implicancias financieras; de otro lado Smith et al (2019) indican que le cibercrimen afecta negativamente el precio de las acciones, pero solo en un periodo de tiempo específico y los consumidores se afectan cuando se tiene acceso a su información financiera, en la misma linea de Kamiya et al. Previamente Sinanaj et al (2013) ya habian indicado que la afectación reputacional afecta a todas las empresas, no solo a las financieras, esto se refuerza con lo planteado por Walden et al (2020) sobre datos médicos.

Wilding (2016) referencia a Gary Warzala hablando sobre la ciberresilencia "Cyber resilience comes down to having an organisation of people who are cyber aware, curious, ask- ing the right questions, actively and continually engaged in learning and who are not just ticking the box". Y es que si bien la literatura es consistente en la medida que es necesario tener políticas de ciberseguridad, lo que termina planteando Wilding (2016) es ir mas alla y enfocarnos en la continuidad del negocio (ISO, 2019) en la medida quue siempre va a existir los ataques, pero dependera de como resistimos a dichos ataques que podamos evitar na afectación a la reputación, esto en la línea de lo expresado por Kamiya et al (2021).

> Organizations need to be thinking about cyber resilience not just cyber security. Cyber resilience can be described as the ability of any organization to prevent,

> detect, respond and recover from the impacts of an attack with minimal damage to their reputation and competitive advantage. (Wilding, 2016)

Corradini (2020) plantea ademas que para una adecuada medición de la afectación de la reputación corporativa tras una brecha de seguridad, se debe incluir la protección de datos personales como indicador relevante. Lehude (2019) tambien se alinea con esta idea.

El ocultamiento y los humanos

Amir et al (2018) plantean que se tiene menos información sobre la real dimensión de los ciberataques porque no se declaran para evitar el impacto reputacional. Aún la medida que existen obligaciones legales para revelar la información (en especial en Europa y América Latina asociados a temas de protección de datos personales (European Union, 2016; OEA 2018; OEA 2019)) o ligados a temas de sistemas financiero, la información puede ser ocultada/retenida hasta que es inminente su descubrimiento. En un esfuerzo por reducir el cibercrimen, muchos estados (de USA) han adoptado leyes de divulgación de violación de datos (también conocida como notificación de violación de seguridad), que requieren que las empresas notifiquen a las personas cuando su información personal se ha visto comprometida.(Romanosky et al, 2011)

Sobre la relación entre las posibilidades de descubrimiento y la ocultamiento, Amir et al (2018) encuentran que las firmas que ocultan información (la retienen) tienen menos cobertura de analistas, un gobierno corporativo más débil y un menor riesgo de litigio que las firmas que revelan/divulgan, en la misma línea avanzan Kamiya et al (2021).

> The proportion of the market reaction to withheld and disclosed cyber-attacks also implies managers disclose cyber-attacks only when investors already suspect that, with a 40% chance, an attack has occurred. When the likelihood of independent discovery by external parties is lower, managers withhold the information. Overall, our analyses suggest voluntary disclosure of cyber-attacks

> is rare. If regulators wish to ensure information on cyber-attacks reaches investors, they should consider imposing stricter mandatory disclosure rules regarding cyber-attacks and clearer materiality thresholds. (Amir et al, 2018)

Ali et al (2021) parten de la premisa que los incidentes de seguridad no son tan frecuentes pero qe tienen alto impacto los que si son, en contra partida de Amir et al que plantea que son frecuentes pero no se divulgan.

Ali et al (2021) hacen un extenso análisis desde las metas del desarrollo sostenible, en especial para firmas de carácter público, pero llega a la conclusión de la poca existencia de los casos; aunque revela que pudiera haber tambien un especial impacto en los inversores de corto plazo, sin embargo ss conclusiones nos hacen pensar que se parte de una premisa de no ocultamiento de información porque estan en bolsa, cuando se ha visto en otros artículos, como en la realidad, que se oculta información precisamente para evitar la afectación en el mercado.

> The adverse economic effects of ISec breaches and the lack of proof of a successful turnaround reinforce the need to pay careful attention to the threat of ISec breaches. Today, information systems are conceivably more vulnerable to ISec breaches than they were previously. While serious ISec breaches are not common, they can seriously hinder a firm's stock performance and decrease investor confidence in the years ahead. Firms must do whatever they can to avoid significant intrusions of ISec and reduce the extent of the breach of ISec. Moreover, companies must establish the ability to anticipate ISec breaches, including the detection, classification, and oversight of any ISec compliance incidents affecting internal processes, vendors, and customers. (Ali et al, 2021).

Cabe destacar que en un país con un menor cantidad de empresas de acciones públicas no significa que tenga menor cantidad de impacto sobre el valor de la compañía sino que el análisis de brechas debe realizarse de otra manera.

Hemos de añadir que el factor humano en todo este proceso es clave, pero ha ido perdiendo su presencia. La decisión de revelar o no revelar no es de una

inteligencia artificial sino de una persona, pero a su vez también son personas los elementos mas disimiles en los procesos de ciberseguridad, más cuando se trata de crear una cultura de ciberseguridad en las organizaciones. “Una cadena es tan fuerte como el más débil de sus eslabones”.

Corradini (2020) es clara en mostrar este enfoque, no solo se trata de cambiar la aproximación desde la tecnología sino entender que el eje del proceso es el ser humano que toma las decisiones en base a la tecnología. Finalmente

> In handling cybersecurity risks, we should not forget the central role played by humans and their relationship with digital technologies. We do not want to criminalize technologies, but it is a fact that we are becoming less and less autonomous in taking decisions and our tendency is to rely more and more on technology.
>
> Differently from the past, we are now dealing with powerful technologies, such as Artificial Intelligence, on which we have even less control. In this sense, lack of human control can represent a new serious problem, affecting security, too. In addition, ethical and social questions have to be faced, since these technologies have a significant impact on our lives.
>
> It is time to change our approach to cybersecurity radically, and to consider the human factor in the right perspective. People are considered the weakest link in the security chain, since most data breaches and incidents involve human element. Instead, humans can become the strongest link for any organization when they are well-trained and motivated to participate to security activities. (Corradini, 2020)

Y ¿que ocurre cuando los datos no son financieros, en especial cuando los datos son medicos? Si bien hemos recopilado información sobre como se oculta información para evitar las repercusiones financieras (Ali et al (2021), Kamiya et al (2021), Romanonsky et al (2011), Amir et al (2018)), a veces la información filtrada no es financiera pero tambien puede generar una afectación reputacional a una

organización, este es el caso de los datos médicos, pero al igual que en lo referenciado a casos generales en estos casos son los oficiales de seguridad quienes tienen a no revelar las brechas, por la sensibilidad de la información y la afectación reputacional a la organización (Walden, 2020).

Conclusiones

El desarrollo de la tecnología digital ya va mas de 80 años, el internet ya tiene mas de 50 años y en América Latina en general mas de 30 en promedio; sin embargo los analisis sobre la utilización de la red en general para los negocios se han ido enfocando en el ambiente del B2B y el B2C, como instrumendo de producción, como herramienta en si mismo, dejando de lado los peligros que pudieran acarrear el uso de dicha tecnología, ya no solo para la propia empresa sino para la información de los consumidores. Los diversos artículos referenciados ademas ahondan en las implicancias de una gestión inadecuada de las brechas de seguridad en la reputación de la organización y su afectación en su valor de mercado.

Y es aquí donde los diversos artículos toman el fenómeno desde diferentes aristas que a su vez nos obligan a poder tomarlos en conjunto para formarnos una imagen completa. La mayoría de los análisis parten de brechas declaradas o conocidas, cuando es alto el porcentaje de casos que no se revelan, es más se ocultan y en el mejor de los casos se hacen públicos ya en ultima ratio.

Una segunda premisa es que la obligación de declarar las brechas, más cuando afectan datos personales, esto tiene una implicancia alta en lugares donde la legislación es mandatoria y sancionadora pero aún allí prefieren no revelar las brechas o asumir las sanciones, a tener que revelar a sus consumidores las afectaciones, salvo que no sean recuperables.

Un tercer elemento a considerar es que muchas veces no son los usuarios quienes generan el temor, porque las ventas se pueden reestablecer en el largo plazo (inclusive en el corto), mejorando la relación con el consumidor o aumentando los niveles de control; el real problema son los accionistas/inversores que tienen mayor

impacto sobre la empresa al cambiar su percepción sobre la seguridad de la información en la organización y por ende afectando el valor de las acciones (sobre todo en empresas que cotizan públicamente). Ciertamente que en países donde la cantidad de empresas en bolsa es muy pequeña esto resulta siendo de poco impacto global, o donde no estan obligadas a mostar las brechas, o donde inclusive debiendo mostrarlas no lo hacen. Es conocido que el ecosistema minero peruano ha sido afectado por diversas brechas de seguridad pero ninguno de esos casos ha sido declarado públicamente.

Como cuarta conclusión la idea que el ecosistema se puede afectar con la brecha de una de las empresas es importante, “Barbam propinqui radere, heus, cum videris, prabe lavandos barbula prudens pilos”, si ves que esta pasando algo en la casa del vecino es probable que pase en tu casa, por lo cual la construcción de redes de información de empresas en el mismo ecosistema es mas que necesario, aún cuando fueren competidores directo, porque las brechas de uno afectan la percepción de consumidores e inversores.

Una quinta idea se plantea desde lo que implica la inversión en ciberseguridad de manera preventiva frente a la reactiva; la primera ayuda al crecimiento y preparar la organización para la continuidad de negocio frente a incidentes, la segunda puede implicar reducción de “toma de riesgo” del negocio e inclusive reducción de inversión en I+D frente a aumento de inversión en cibereguridad.

Finalmente, la revisión de la literatura muestra información sobre USA fundamentalmente, dejando bastante notoria la falta de información sobre América Latina, siendo una oportunidad de desarrollo de investigación.

Referencias

AlGhamdi, S., Win, K.T & Vlahu-Gjorgievska, E.(2020). Information security governance challenges and critical success factors: Systematic review. *Computers and Security*, 99. https://www-sciencedirect-com.ezproxybib.pucp.edu.pe/science/article/pii/S0167404820303035?via%3Dihub

Ali, S.E.A., Lai, F.-W., Hassan, R., Shad, M.K.(2021)The long-run impact of information security breach announcements on investors' confidence: the context of efficient market hypothesis. *Sustainability (Switzerland),* 13(3), 1-27

Amir, E., Levi, S., Livne, T. (2018).Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23 (3), 1177-1206.

Andoh-Baidoo, F.K., Amoako-Gyampah, K., Osei-Bryson, K.-M. (2010). How internet security breaches harm market value. *IEEE Security and Privacy*, 8(1) 2010, 36-42

Asia-Pacific Economic Cooperation (2005). *APEC Privacy Framework*. APEC.

Bandara, R., Fernando, M., Akter, S. (2020). Addressing privacy predicaments in the digital marketplace: A power-relations perspective*. International Journal of Consumer Studies*, 44 (5), pp 423-434. https://onlinelibrary-wiley-com.ezproxybib.pucp.edu.pe/doi/full/10.1111/ijcs.12576

Barnett, M., Jermier, J. & Lafferty, B. Corporate Reputation: The Definitional Landscape. *Corp Reputation Rev* **9,** 26–38 (2006). https://doi-org.ezproxybib.pucp.edu.pe/10.1057/palgrave.crr.1550012

Baloyi, N., Kotzé, P. (2020) Data privacy compliance benefits for organisations – A cyber-physical systems and internet of things study. *Communications in Computer and Information Science 1166* CCIS, pp. 158-172

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004) The effect of internet security breach announcements on market value: Capital market reactions for breached

firms and internet security developers. *International Journal of Electronic Commerce*, 9 (1), 70-104. https://www-tandfonline-com.ezproxybib.pucp.edu.pe/doi/abs/10.1080/10864415.2004.11044320

Choong, P., Hutton, E., Richardson, P.S. and Rinaldo, V. (2017), "Protecting the brand: evaluating the cost of security breach from a marketer's perspective", *Journal of Marketing Development and Competitiveness*, 11(1).

Corradini, I. (2020) Building a Cybersecurity Culture in Organizations: How to Bridge People and Digital Technology. Springer.

Corradini, I. (2020). Is Data Protection a Relevant Indicator for Measuring Corporate Reputation?. *Advances in Intelligent Systems and Computing*, 1219. https://link.springer.com/chapter/10.1007/978-3-030-52581-1_18

Eling, M.,McShane, M., Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24, 93-125

European Union (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

Fombrun, C., van Riel, C. (1997) The Reputational Landscape. *Corp Reputation Rev* 1, 5–13 (1997). https://doi-org.ezproxybib.pucp.edu.pe/10.1057/palgrave.crr.1540008

He, C.Z., Frost, T., Pinsker, R.E. (2020). The impact of reported cybersecurity breaches on firm innovation. *Journal of Information Systems*, 34(2),187-209

Hillenbrand, C., Money, K. (2007). Corporate responsibility and corporate reputation: two separate concepts or two sides of the same coin? *Corporate Reputation Review* 10(4), 261–277

International Stardards Organizacion (2018). *ISO 27001:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary.* ISO.

International Stardards Organizacion (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.* ISO.

International Telecommunications Union (2010). *Definition of cybersecurity.*

International Telecommunications Union (2010). *Resolución 181 (Guadalajara)*

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., Stulz, R.M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, 139(3), 719-749

Lehuede H. (2019) *Corporate governance and data protection in Latin America and the Caribbean.* CEPAL. LC/TS.2019/38.

Lehuede H. (2020). *Cybersecurity and the role of the Board of Directors in Latin America and the Caribbean*. CEPAL. LC/TS.2020/103

Organización de Estados Americanos (2018*). State of Cybersecurity in the Banking Sector in Latin America and the Caribbean.* OEA.

Organización de Estados Americanos, Amazon Web Services (2019). *Cibereguridad: Marco Nist. Un abordaje integral de la ciberseguridad*. OEA

Organización de Estados Americanos, Internet Security Alliance (2019). *Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas*. OEA

Romanosky, S., Telang, R., Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft?. *Journal of Policy Analysis and Management*, 30(2), 256-286

Sinanaj, G., Muntermann, J. (2013). Assessing corporate reputational damage of data breaches: An empirical analysis. *26th Bled eConference - eInnovations: Challenges and Impacts for Individuals, Organizations and Society, Proceedings 2013*, 78-89

Smith, K.T., Jones, A., Johnson, L., Smith, L.M. (2019). Examination of cybercrime and its effects on corporate stock value*. Journal of Information, Communication and Ethics in Society*, 17(1), 42-60

Veh, A., Göbel, M., Vogel, R. (2018). Corporate reputation in management research: a review of the literature and assessment of the concept. *Business Research*, 12(2), 315–353

Walden, A., Cortelyou-Ward, K., Gabriel, M.H., Noblin, A. (2020). To report or not report health care data breaches. *American Journal of Managed Care,* 26(12), E395-E402

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people?. *Business Information Review*, 33(2), 94-99

World Economic Forum (2017) *Advancing Cyber Resilience Principles and Tools for Boards*. WEF.