ALEKSANDRA HĘĆKA-SADOWSKA
KRZYSZTOF ŁYSKAWA
https://doi.org/10.33995/wu2023.2.3
data wpływu: 26.04.2023
data akceptacji: 06.07.2023

Operational Cyber Risk in the differing business model of Insurance Companies: the example of Poland

Cybersecurity has become one of the greatest challenges in today's post pandemic, digital and interconnected world, and also a subject of strategic importance for the insurance industry. There is no doubt that the advance of technology and the increased use of big data and cloud computing have set up an opportunity for insurance business, but they also expanded insurance companies' vulnerabilities towards cyber risk. As insurers collect a large amount of confidential data, including protected personal sensitive information, they are a natural target for cyber-attacks. On the one hand, the aim of the article is to indicate how the risks associated with digitalisation affect the day-to-day operations in selected business areas of an insurance company, and which methods may be used to manage them, on the other. After a general review of cyber risk based on recent branch reports and survey results, the authors identified its global economic impact with particular regard to financial institutions, and also insurers' exposure and perception of cyber risk and cybersecurity spending. Moreover, administrative decisions issued by the President of the Personal Data Protection Office in Poland, selected jurisdictions and loss scenarios for insurance companies were examined with a deeper dive into underwriting, selling, administration and claims handling processes. The results of the literature study show that cyber risk is recognized to be one of the most significant non-financial risks (in terms of the source, not result of the risk) for insurers and that many proactive security measures can be implemented. However, due to the high vulnerability to leaks of confidential personal and financial data or unauthorized system access, which may cause not only financial loss, but also business interruptions and reputational damage, in the authors' opinion, loss prevention and reduction are insufficient. Thus, both insurance and non-insurance methods of external financing cyber risk results were indicated. On this basis, the cyber insurance is considered by the authors to be the best tool providing both prevention and financial compensation in case of cyber incidents, also in insurance companies.

Keywords: cyber risk, operational risk, insurance company, risk management, cyber insurance

Operacyjne ryzyko cybernetyczne w odmiennym modelu biznesowym zakładów ubezpieczeń na przykładzie Polski

Cyberbezpieczeństwo stało się jednym z największych wyzwań dzisiejszego postpandemicznego, cyfrowego i połączonego świata, a także tematem o strategicznym znaczeniu dla branży ubezpieczeniowej. Nie ma wątpliwości, że postęp technologiczny, w tym zwiększone wykorzystanie dużych zbiorów danych i przetwarzanie ich w chmurze stwarzają możliwości dla branży ubezpieczeniowej, ale także zwiększają podatność zakładów ubezpieczeń na ryzyko cybernetyczne. Ponieważ ubezpieczyciele zbierają duże ilości poufnych danych, w tym dane osobowe, są naturalnym celem cyberataków. Celem artykułu jest wskazanie z jednej strony, w jaki sposób zagrożenia związane z digitalizacją wpływają na codzienne funkcjonowanie zakładu ubezpieczeń w wybranych obszarach, a z drugiej jakie metody mogą służyć zarządzaniu nim. Po ogólnym przeglądzie ryzyka cybernetycznego na podstawie ostatnich raportów branżowych i wyników badań, autorzy zidentyfikowali jego globalny wpływ ekonomiczny ze szczególnym uwzględnieniem instytucji finansowych, a także ekspozycję i postrzeganie ryzyka cybernetycznego przez ubezpieczycieli oraz wydatki ponoszone na cyberbezpieczeństwo. Ponadto zbadano decyzje administracyjne wydane przez Prezesa Urzędu Ochrony Danych Osobowych w Polsce, wybrane orzeczenia i scenariusze szkodowe dla zakładów ubezpieczeń ze szczególnym uwzględnieniem procesu underwritingu, sprzedaży, administracji i likwidacji szkód. Wyniki badań literaturowych wskazują, że ryzyko cybernetyczne uznawane jest za jedno z najistotniejszych ryzyk niefinansowych (w kontekście źródła zagrożenia, a nie rezultatu) dla ubezpieczycieli, a także że dostępnych jest wiele proaktywnych środków bezpieczeństwa, które mogą oni wdrożyć. Jednak ze względu na dużą podatność na wycieki poufnych danych osobowych i finansowych lub nieautoryzowany dostęp do systemu, który może spowodować nie tylko straty finansowe, ale także przerwy w działalności i szkody wizerunkowe, zdaniem autorów zapobieganie i ograniczanie strat jest niewystarczające. Wskazano więc zarówno ubezpieczeniowe, jak i poza ubezpieczeniowe metody zewnętrznego finansowania skutków cyber ryzyka. Na tej podstawie cyber ubezpieczenie jest uważane przez autorów za najlepsze narzędzie zapewniające zarówno prewencję, jak i kompensację strat spowodowanych realizacją operacyjnego ryzyka cyber również w zakładach ubezpieczeń.

Słowa kluczowe: cyberryzko, ryzyko operacyjne, zakład ubezpieczeń, zarządzanie ryzykiem, ubezpieczenie cyber

DR ALEKSANDRA HĘĆKA-SADOWSKA – Poznań University of Economics and Business
e-mail: aleksandra.hecka-sadowska@ue.poznan.pl
ORCID:0000-0002-7649-9528

DR HAB. KRZYSZTOF ŁYSKAWA – Poznań University of Economics and Business
e-mail: Krzysztof.Lyskawa@ue.poznan.pl
ORCID: 0000-0002-7409-8624