News

Insurance in focus: the advance of technology, the acceleration of innovations and the threat of cyber risks

Written by: Ronaldo de Andrade - 11/08/2022

Brazil is making great strides towards insurance innovation based on use, consumption, and user experience, a scenario that is strongly driven by the technological day-to-day of modern life, which is changing standards and creating new market needs.

If on the one hand this transformation movement that we are experiencing and building opens infinite possibilities and a fertile path for innovation, on the other hand cyber-attacks are currently a real and representative risk that requires preventive and mitigating actions by companies (and people!).

Data intelligence in the field

The effects of technology are everywhere. In the field, the advance of high-speed networks – through 5G connectivity – is making crops smarter and more dynamic.

The use of IoT, the so-called “Internet of Things”, technology used to integrate devices to the internet, as well as the use of historical data for decision making (varieties planted, best times for planting and cutting, among others), increase the chances of success of the sector’s entrepreneurs.

On the other side, consumers are also benefited by technological advances, with a greater availability of products and lower costs, resulting from a more intelligent production and storage, which optimizes the flow of national production.

All this integration and connectivity broadens horizons, bringing concrete possibilities of customized insurance to reflect the reality of the field, but it also amplifies risks in the virtual environment, and those who are not alert are doomed to large-scale losses.

This is because smart, autonomous networks necessarily need to be resilient and adequately protected from growing and increasingly sophisticated cyber-attacks.

According to an FBI alert for the agribusiness sector containing five examples of companies attacked by cybercrime, one farm located in the United States suffered financial damage of $9 million due to a temporary systems shutdown.

The loss stemmed from a ransomware attack, in which an unknown group gained access to the farmer’s internal network using compromised credentials. The incident, which occurred in January 2021, is one of the worst impacts of ransomware attacks cited by the US research department.

Innovation in Health Insurance

Another sector heavily impacted by technology, healthcare has made significant advances in the use of data intelligence. More and more gadgets collect data and references from our body, such as heartbeat readings, exercise levels, stress, and sedentary lifestyles, for example, bringing important parameters to the medical field, health plans, and operators.

Imagine health insurance where the monthly cost decreases or increases based on this data that is collected in real time regarding your health and physical activity level? Operators are eyeing this new market, which is already a reality. According to a study conducted by Check Point Research (CPR) in early 2022, Healthcare was the second most cyberattacked sector in the period 2020 to 2021. Second only to the retail sector, healthcare institutions and their platforms have seen a 64% increase in attacks in Brazil.

In December 2021, the ConecteSUS platform, which issues the covid-19 vaccination certificate, went offline after the Ministry of Health was the target of a hacker attack. The platform was down for 13 days, affecting millions of Brazilians who used the service to prove their vaccination.

The risks of connected cars…

What if your car had full connectivity with auto insurance carriers, with 5G facilitating the transmission of route, driving mode, time in transit, and most importantly, driving safety? These are parameters that are constantly being collected and companies are in the process of evaluating and flexing their insurance bill month by month.

On the other hand, there are several scenarios in which drivers can fall victim to attacks that threaten their safety in connected cars.

The research “Cyber Security for Connected Cars: Exploring Risks in 5G, Cloud and Other Connected Technologies,” published by cybersecurity consultancy Trend Micro, evaluated 29 real-world cyberattack scenarios in the DREAD 1 threat model in a qualitative risk analysis targeting connected cars, which proved vulnerable ?because they are easily discovered.

In this type of cybercrime, the attack can be launched against or from the vehicle, and more than 17% of all variables analyzed were considered high risk, as they proved to be of low complexity for attackers, who do not require deeper knowledge of connected car technology, and can be exploited by attackers with little skill.

Technology and its impact on the insurance industry

All this technology, which is already a reality, puts us in a new insurance model that is not based on average or standard, but on the individuality of each insured.

At this very moment, thousands of data are being connected and collected on your smartphone or any other device through which you are reading this article. In this new market where data is the core product of many solutions, the care with connectivity and respect for privacy regulations, such as the General Law of Data Protection (LGPD), are fundamental points of any activity that involves

technology and services.

Measures based on data models for qualitative and quantitative risks are already indispensable if the market is to keep up with this development.

Horiens, through its Risk Labs, has a track record of probabilistic risk modeling in complex areas such as supplementary health, agricultural productivity, collateral default and operational continuity.

This work is done by developing and validating quantitative models to support our clients' strategic and tactical decision-making, providing the necessary security for the company to innovate and grow in a sustainable way.

Let's schedule a chat about this topic? Contact contato@horiens.com