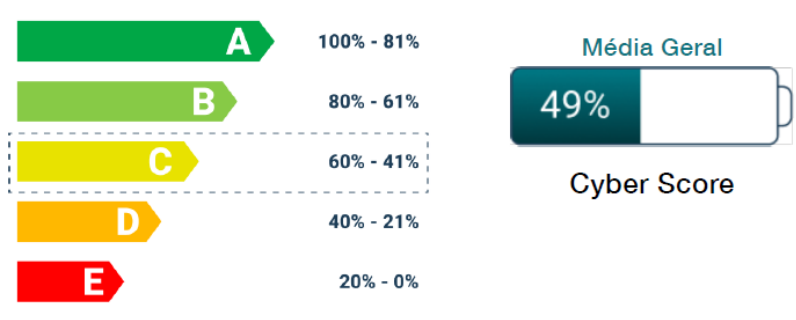
The biggest Brazilian Companies get grade 5 under 10 in unprecedented research about Cyber Security

Most companies (93%) have mechanisms to detect cyber-attacks, however, 42% do not have a cybersecurity incident response plan



The Cyber Score methodology, developed and patented by SDL, is based on the main global security regulations and best practices.

SãO PAULO, SP, BRAZIL, September 19, 2023 /EINPresswire.com/ -- The first study in Brazil to assess the maturity of publicly traded companies (with shares listed on B3) in cybersecurity was released this Wednesday (13), at an event at Insper's headquarters in São Paulo, revealing that a portion of the largest companies in the country are far from the recommendations and best practices indicated by the leading global cybersecurity agencies. The Cybersecurity Sector Research was developed in an unprecedented way by the Brazilian Association of Public Companies (Abrasca) and The Security Design Lab (SDL) – a global cybersecurity research and development network operating in South America and Europe – using the Cyber Score methodology, which measured the responses of the 109 participating companies from the following sectors: Agribusiness, Education, Energy, Engineering, Financial, Industry, Oil & Gas, Health, Services, Technology, Telecommunications, and Retail. The average score was 4.9 on a scale of 0 to 10, which indicates an intermediate degree of maturity.

The assessment, with 86 questions segmented into 12 chapters was administered between the months of May and August this year. The Cyber Score methodology is already used by several companies globally and this is the first application in a sectoral survey.

Based on the collected data, Abrasca aims to support publicly traded company’s technical and compliance areas to disseminate the subject's relevance among C-levels, boards of directors, and shareholders. “The importance of the topic in the capital market is growing and there is no turning back. It stopped being an IT problem and became a problem for all companies, public or not. The world is moving towards regulations that are more appropriate to the new reality and better practices, hence the importance of having updated data to understand where we are and,

therefore, guide the discussion 'with our feet on the ground', in a pragmatic and efficient way", says Pablo Cesário, Abrasca Executive President.

Best Ranked

The companies that achieved the highest cybersecurity compliance rates are from the Industry/Manufacturing, Telecommunications, Oil & Gas, and Financial sectors. According to those who applied the research, there is no cut-off score when information security is analyzed, as each company and sector has particularities. However, a rating of 7.5 is already considered very good.

"The score of 5 out of 10 obtained in the general average shows a lot of room for improvement, but this is a scenario that is not inconsistent with what global research indicates. Complying with cybersecurity recommendations and best practices helps companies establish protection measures, reducing their area of exposure against potential attacks", points out Alexandre Vasconcelos, Latin America Director, at The Security Design Lab.

The Abrasca and SDL report points out that, on the one hand, 93% of companies have some mechanism to detect cyber-attacks and 65% say they can identify and act in response to incidents to ensure the business continuity and its functions. On the other hand, 42% do not have a cybersecurity incident response plan, 65% do not guide the team to deal with and respond to cybersecurity incidents and 73% do not have access control mechanisms for the OT system (Operational Technology) and ICS (Industrial Control Systems). By comparison, the latest America's Most Cybersecure Companies survey carried out by Forbes with 200 American companies identified that only 30% of them have a Chief Information Security Officer (CISO), while the Brazilian survey showed that this number is higher, reaching 58% in the country.

The Supply Chain has been growing as a preferred target for cybercriminals. Some attacks directly impact the chain, such as the one at Solar Winds, affecting more than 18 thousand companies. "A company can have its operations affected, without having been the direct target of an attack. The research shows us worrying data, where 52% of companies do not implement risk management for this chain", warns Vasconcelos.

Attacks and costs rise for companies in the world

The costs of cybercrime to the global economy are expected to jump from US$3 trillion per year in 2015 to US$10.5 trillion in 2025, according to a survey prepared by Howden, an independent multinational insurance company. Regarding the frequency of cyber-attacks worldwide, the company analyzed data from the NCC Group and identified that, in the first five months of this year, compared to the same period in 2022, there was a 48% increase in the number of ransomware-type attacks (hijacking of data with ransom charge). According to research by Verizon (2023), around 83% of breaches involve actors external to companies, with 95% of attacks being motivated by financial issues and the highest rate of external attacks coming from organized crime.

Also, according to a global survey by Howden, the equivalent of R$247 million was paid in claims

for incidents related to ransomware in the last three years, with the healthcare sector being the most affected, followed by retail, finance, and services companies. In Brazil, according to the company, incidents in which insurance policies were activated resulted in the payment of expenses between R$2 million and R$65 million, compared to claims made in the local market.

“We are discussing an issue that affects not only the company's market value but also puts business continuity into question. And even more so, it is being reflected in the company's capital cost. We are already seeing an increase in the cost of credit operations due to this issue, as well as the review of ratings from rating agencies considering cybersecurity analysis”, says Rafael Sasso, coordinator of CINC – Abrasca's Corporate Innovation Commission.

Cybersecurity Sector Research Main Results

- 93% of companies have mechanisms to detect cyber-attacks;
- 42% do not have a cybersecurity incident response plan;
- 38% of companies do not have a regular information security training program;
- 65% of companies do not guide staff to deal with and respond to cybersecurity incidents;
- 42% of companies do not have a CISO or similar position (executive responsible for information security);
- 46% of companies do not have an information security committee;
- 51% do not have a business impact analysis;
- 40% do not have a business continuity

Marcelo Dias
Ryto Public Affairs
+55 11 98568-1381
email us here