Cyber Attack in COVID-19 period: protecting business to preserve results

2020 reported, with COVID-19 pandemic, a huge increase in cyber attacks and beginning of 2021 is showing the same trend. Increased cybersecurity risks emerged due to changes in way companies were (and are) obliged in doing business. Some examples are related to data breaches, fraud, hacking, video-and teleconference hijacking.

2Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

Cybercrime is one of the most disruptive and economically damaging criminal activities. Not only does it cause substantial financial damages and pose a serious threat to society and the global economy, it also has indirect effects in undermining the public's confidence in digital transformation and overall trust in technology (INTERPOL, World Economic Forum). World Economic Forum is estimating cyber crime third economy in the world after Us and China.

CRIF
Together to the next level

Cyber Attack in COVID-19 period: protecting business to preserve results

It means than more than in the past the cyber risk level must be considered when a company's overall risk analysis is done.

As already underlines before Covid-19 pandemic, but now with a dramatically evidence, no business is safe, regardless of size, industry, market or country. Understanding in advance if a partner or a potential partner could be at risk is mandatory for every company. A cyber-attack or a data breach causes business and reputational damages, as well as regulatory and compliance issues.

If we consider data breach only, top sector with the highest cost per industry are healthcare, energy, financial services, pharma, technology, manufacturing, services, entertainment and education. With healthcare with a 10.5% 2020 vs 2019.(IBM Ponemon Cost of Breach Study).

The FBI recently reported that the number of complaints about cyberattacks in US to their Cyber Division is up to as many as 4,000 a day. That represents a 400% increase from what they were seeing pre-coronavirus. Interpol is also seeing an "alarming rate of cyberattacks aimed at major corporations, governments, and critical infrastructure." These attacks are targeting all types of businesses but large corporations, governments, and critical medical organizations have been major targets.

CRIF
Together to the next level

www.skyminder.com

Cyber Attack in COVID-19 period: protecting business to preserve results

In such scenario, one of the most critical area impacted by cyber attack is supply chain.

The supply chain is a system of activities in handling, distributing, manufacturing and processing goods in order to move resources from a vendor to a consumer. Due to the complexity and importance of the supply chain, businesses must be vigilant in protecting it against a cyber-attack. A supply chain cyber-attack has the potential to damage less secure elements in the supply network and can occur in any industry, from financial sectors to manufacturing and government.

The threat of a supply chain attack is significant in modern organisations. Globalisation, decentralisation and outsourcing of supply chain activities has created increased potential for damage to all linked entities in the case of a cyber-attack. Sharing information digitally with suppliers is a vital process but it is this digital connection that can leave businesses exposed to cyber-risk.

The effects of a cyber-attack on a supply chain can be immense and grow quickly. Starting with a major disruption of manufacturing processes, lost revenues, market share reduction and competitive advantage it can then lead to loss of sensitive customer information.

CRIF
Together to the next level

Cyber Attack in COVID-19 period: protecting business to preserve results

This can generate a low level of brand credibility and reputation leaving a company unable to meet requests coming from customers, so customers move to new suppliers able to guarantee provisions. In addition, for customers already using these suppliers it can mean the slow down of their processes with severe internal and external impacts too.

Sadly a cyber-attack not only impacts suppliers as victim of the attack itself but also customers who find themselves having to source a new supplier which isn't always a simple and quick task.

For these reasons it's important businesses understand in advance if a partner or potential partner are vulnerable to a cyber -attack. It's standard practice to analyse business partners from a financial point of view, but now more than ever it's crucial to understand the cyber risks the company may face as well.

This is the reason why SkyMinder, the CRIF platform for the business information where all B2B trade risks are extensively and strategically evaluated across global markets, has made available a KYND Cyber Risk Report. KYND utilises pioneering cyber risk technology and expertise to show simply and easily the cyber risks a company faces. KYND is a UK organisation focused on cyber risk with CRiF as a major shareholder in the company.

CRIF
Together to the next level

www.skyminder.com

Cyber Attack in COVID-19 period: protecting business to preserve results

The KYND Cyber Risk Report is applicable to any kind of business, and requires only a website and company name to quickly show the cyber risks of a business partner.

The KYND Cyber Risk Report can be obtained via SkyMinder which delivers the best information on any existing company around the world, covering 230 countries and territories to support any business decision with the tools to evaluate partners to avoid threats from credit and financials, to anti-money laundering and bribery to cyber-crime.

About KYND
Founded in
February 2018 and headquartered in London, KYND is a new breed of cyber company. KYND makes complex cyber risks simple to understand and manage for every organization, regardless of size, means or industry sector.

CRIF
Together to the next level

www.skyminder.com