Why cyber security is a strategic topic for Boards?

Startups are not immune to cyberattacks and, as large companies, they have a lot to lose: customer lists and records, pricing model, business plans, contracts, social security and credit card numbers, intellectual property... “More than half of all cyber-attacks are now directed at small businesses, according to a 2017 cybersecurity report by the Ponemon Institute.”

A Government survey conducted last year, as part of the National Cyber Security Program, revealed that 66% of cyberattacks occurred in SMEs, 45% occurred in micro businesses and 41% in large companies. https://magazine.startus.cc/data-shows-3-5-smes-experienced-cyber-attack-12-months/ . As explained in this article, the main reasons are: more connectivity, the rise of BYOD (Bring Your Own Device) in the workplace, as well as Internet of Things.

How do cyber-criminals hack small business startups? Here's what we learned from Microsoft https://eu.usatoday.com/story/money/usaandmain/2018/10/17/microsoft-store-cybersecurity-hack-demo/1664184002/

Apollo, a sales engagement startup boasting a database of more than 200 million contact records, has been hacked. Apollo may also face action from European authorities under GDPR. https://www.wired.com/story/apollo-breach-linkedin-salesforce-data/

Cyber criminality is an increasing threat resulting from the complexity of an interconnected business ecosystem and the rapid evolution of technology.
Startups are even more exposed, because they are often more focused on their customers, and delivery of products & services at a low cost, than on administration and security (that they considered as a cost).
Whatever the size of the company, cybersecurity is a major issue for businesses: a cyber risk is a business risk!
Indeed, cyber incidents may impact the systems allowing to sell, to produce or to administrate. They may also impact the critical information of a company and consequences are economic: loss of intellectual property, impact on reputation in case of loss of sensitive customer data, sabotage, fraud and financial losses.

This is why it is a strategic issue for the board of directors and managing directors!

Cyberattack issues can be major, and board members should not wait for an attack to assess the cyber risks and check the implementation of some basic measures to mitigate these risks: for instance, ransomwares hit a number of organizations, holding data hostage by encrypting it and demanding that the organization pay in order to have the data restored. If the organisation has insufficient backups or the backup is also encrypted, the only way to restore the data may be to pay the ransom. In some cases, the decision to pay a ransom may need to be a board-level decision or at the very least discussed.

Too many business leaders believe that cybersecurity is the responsibility of the IT services provider, whereas it is a cross-cutting issue that also concerns customer relations, suppliers,

production systems, maintenance, legal and finance. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Consequently, it is recommended, depending on their business and size of the company, to:
- Put cybersecurity at the forefront of agendas on boards, to be able to identify the most important threats and understand the strategy to put in place to address them (competences, procedures, training, tools…)
- Have at least one board member able to identify and control cyber-risks
- Establish a transparent and regular dialogue between IT managers, executives and board members
- Identify the critical data of the company and find a way to protect them
- Be aware of non-compliance risks (GDPR) with personal data, in particular for B to C businesses

Cybersecurity and data privacy are among the risks that must be overseen by the board. Board members and managing directors can be held responsible if they have not taken steps to protect the information systems and personal data collected by the company.

Marie de Fréminville
Starboard Advisory
Marie.defreminville@starboard-advisory.com

Starboard Advisory
GOUVERNANCE › FINANCE › PERFORMANCE