BIZCOMMUNITY

Pandemic highlights need for cyber risk management

If small and medium businesses had little appetite for cyber risk management before the coronavirus pandemic, they may have developed one now. Mobilising remote workforces, provisioning the right set of tools, managing the flow of data, keeping it secure and controlling who has access to what has likely to have caused disruptions and headaches at best. At worst, lack of cyber risk management has caused companies to grind to a complete halt.

Douw Gerber, business development manager at Securicom

Douw Gerber, business development manager at IT security services company, Securicom, says that lack of cyber risk management is a factor in the higher incidence of cyber related fraud amongst small businesses during the lockdown. Citing Verizon's Business 2020 Data Breach Investigations Report, he says that about a third (28%) of data breaches this year has involved small businesses.

"There are no controls in place to manage access to and the share of information. Backs ups don't happen when they should. Cybersecurity tools aren't updated as they should be. Employees are using unsecured devices to do their work. People are using third party apps to complete tasks. There is no segregation of duties. Appropriate actions aren't taken when security incidents happen. The list goes on."

Gerber recognises that the IT function in the average small medium-sized business ranges from a one-man-band scenario to a small team that performs a range of tasks, one of which happens to be IT. Without concerted management, small businesses are at a disadvantage when it comes to deciding how to go about investing in IT, what tools they need and how they should be provisioned, managed and governed. The result is bad IT spend, tools that don't get used to their max, poor security and more risks.

He stresses that cyber risk management should form part of the overall risk management strategies of every business.

“The work-from-home scenario that has burgeoned in the wake of the COVID-19 pandemic has dramatically increased companies’ exposure to cyber related threats. Companies are not in control of their data or the devices that employees are using to access company resources. When employees use their own unsecured devices for work, they make for a perfect gateway or point of attack on company networks.

“Companies should know who and what devices are accessing their networks. Restrictions should be placed on what information can be accessed, and employees need to understand what they are and why they are there. It is all part of risk management.”

“We are in a rapidly changing world where technologies are evolving all of the time in increasingly complex operating environments. The Coronavirus pandemic and the plummeting economy are making doing business more challenging than ever. It is becoming increasingly important for small and medium-sized companies to strategically position ICT to build resilience and competitive advantage.”