BIZCOMMUNITY

With technology comes risk

Decision makers in organisations must be cautious not to overlook the significant risks of the fourth Industrial Revolution (4IR) in their eagerness to capitalise on the efficiencies offered by technology.

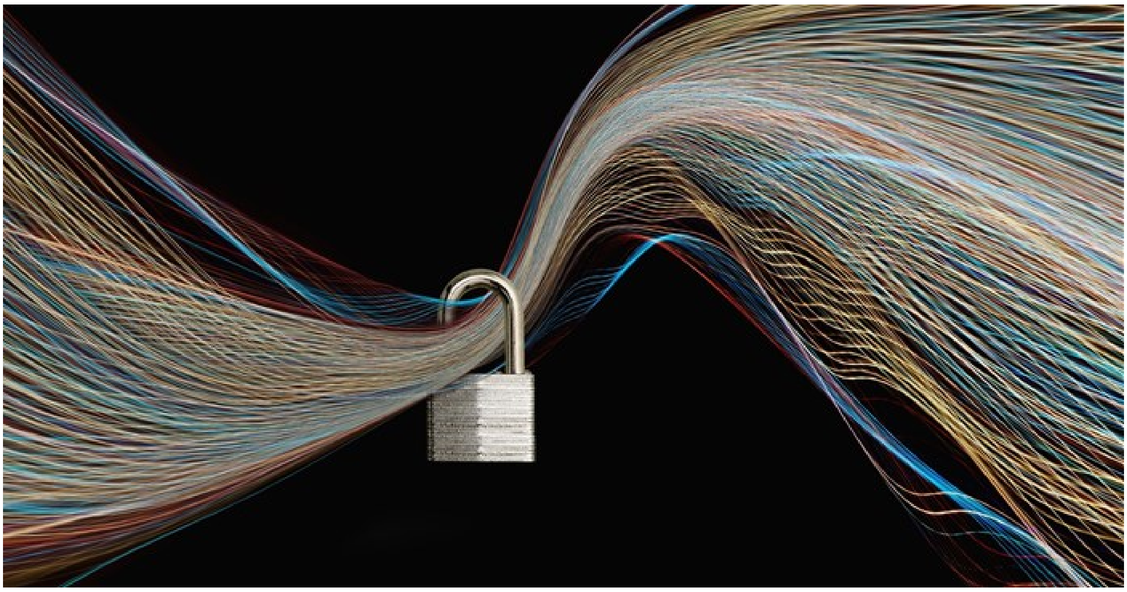

Image source: Getty/Gallo

The potential pitfalls range from external threats like cyber-attacks to internal challenges like employee resistance to job losses brought about by automation, says Tiaan van Schalkwyk, associate director in Deloitte Risk Advisory.

Organisations need to apply their minds now, not at some undefined time in the future.

“Whether it’s something as simple as installing a web-connected doorbell camera or as complex as an automated production line, most South African businesses are already prototyping and even implementing these digital technologies to a greater or lesser extent,” says Van Schalkwyk.

“Companies will have to live with the consequences, good or bad, of these decisions for years, possibly decades. If board members are not on top of how this trend is unfolding in their organisation, they’re abrogating their responsibilities and opening themselves to potential risks.”

Shadow devices

One such hazard comes in the form of shadow information technology (IT) and shadow internet of things (IoT) - information technology and internet-connected devices introduced to organisations in an ad-hoc fashion by line managers or staff members, usually without authorisation.

“Most business leaders are aware of the cyber security and other risks associated with employees’ use of unsecured personal laptops, tablet PCs and smartphones. However, in the IoT era the threat can come in the guise of something as innocuous as a web-connected printer or microwave oven.”

According to Van Schalkwyk, many of these shadow IoT devices, particularly the more affordable models from lesser known manufacturers, are not fit for purpose and expose the organisations in which they are installed to a host of cyber risks. These devices were not designed, or configured out-of-the-box, with security in mind.

These include internet routers, security cameras and other devices that come with default passwords known to hackers or insecure software that cannot be updated with the latest security patches.

“Of course, it is unrealistic to expect boards to be involved in such granular decisions as which model of microwave to buy for the third-floor kitchen in the Bloemfontein branch office. But this example illustrates the importance of putting in place policies and cyber security practices that inform every level of decision making, including local procurement practices," he says.

Automation agitation

As 4IR technology like automation take root and its full implications – particularly in the form of job losses – begin to sink in, another source of potential risk emerges: employee discontent.

“If automation implementation is not managed properly, employee uncertainty may boil over into active resistance to the changes. This situation can be exacerbated as labour bodies and even activist hacker groups (‘hacktivists’) seek to capitalise on these tensions.”

In the short to medium term, as organisations seek to implement automation, Van Schalkwyk advises that the associated issues need to be addressed upfront, particularly as it is usually lower skilled jobs that are the first to be impacted. “Potentially affected staff and labour bodies should be among the first stakeholders you engage with, not the last.”

He adds that if such engagements are to be constructive, a longer-term approach needs to be in place, one that involves both companies and government in coming up with solutions like reskilling employees for other roles within the organisation or for entrepreneurial opportunities outside of the organisation.

War footing

As organisations become increasingly aware of the potentially devastating consequences of cyber-attacks, many are taking out cyber insurance to mitigate the risks.

Van Schalkwyk warns, that few are aware of clauses in many of these insurance policies that may exclude coverage if the cyber attack is found to have originated from a nation state (an act of cyber warfare), as a small but significant minority now do.

He cites the scenario of a bank which may be targeted by hackers backed by a foreign government seeking to test its capability to bring down a target country’s financial system in the event of a future conflict.

“As with the earlier procurement example, it may seem unrealistic to expect the board to interrogate management decisions like insurance in such detail, but this does speak to the importance of tapping into the experience and expertise of trusted, knowledgeable third-party service providers and advisory firms before making decisions of this nature.”

There should also be a comprehensive incident response plan in place, one tailor-made for the organisation's specific requirements and potential vulnerabilities.

More generally, boards need to ensure that organisation-wide processes and procedures are put in place that will ensure that decision makers have full sight of cyber threats and the risks to be managed.

These should include regular reporting which is imperative in identifying the risks, exposing security gaps and ensuring that there are plans in place to address those gaps. This will also help improve accountability for cyber security.

“Make no mistake. The risks are substantial and multi-faceted, but they are not unmanageable. It does, however, require an organisation's leaders to look beyond the hype and approach the matter with discipline and appropriate governance if it is to realise the full value and promise of 4IR,” concludes Van Schalkwyk.