Secure your digital transformation journey with these six tips

By [Quintin McCutcheon](#)   23 Sep 2020

As the world adjusts to a new normal, the current situation has underlined the importance of all things digital to keep the basics of our society running - from power and water services to online shopping, and remote learning to entertainment.

Quintin McCutcheon, Digital Transformation Leader, Schneider Electric South Africa

While digital touchpoints provide vital help in coping with everyday life and mitigate some impact on people's daily lives, the growing connectivity of everything presents challenges on the security front.

Cybersecurity threats are on the rise everywhere, and South Africa is no exception. According to findings from global cybersecurity company, Kaspersky Lab, there was a major spike in network attacks in South Africa earlier this year, where hackers attacked up to 310,000 devices during a one-week period, by far outstripping the weekly average of 20,000 to 30,000.

The country also endured the longest-running cyber-attack campaign in all the regions monitored by Mimecast, with the company detecting more than 116,000 attacks over an eight-day period in July by an unknown actor or group.

The coronavirus pandemic has accelerated the scaling up of technology both in the public and private sectors. In a world where lockdowns have become the norm, digital is the strategy to overcome new challenges. However, in the rush to digital, cybersecurity must not be an afterthought.

Operations can become more vulnerable as large numbers of employees work remotely. The main challenge businesses are facing right now is to maintain a balance between business needs and keeping their organisations safe from threats, while ensuring business continuity.

Business leaders should establish a pragmatic approach and create a multi-layered cybersecurity strategy that will reduce business and digital risk whilst taking into account best practices protecting people, processes and technology.

Here are my suggestions:

1. **Secure your digital ecosystem**

   Understanding digital risk means looking well beyond a sole connected object or database. IT and OT leaders must review all the potential risks across the extended digital enterprise, which includes the supply chain and partners. They then have to craft and communicate a digital risk strategy that will be understood by management.

   I recommend that leaders look to the five-part cybersecurity framework developed by the National Institute of Standards and Technology, which helps organisations identify, protect, detect, respond to and recover from online threats.

2. **Establish end-to-end cybersecurity practices**

   Cybersecurity is not just about your hardware and software. The best approaches with mitigating digital risk take into account people, processes and technologies. When putting together a cybersecurity strategy, organisations must begin with identifying risks across this extended enterprise.

   Take the time to understand where the greatest potential risks are, and what impact any unaddressed vulnerabilities will have on your business. Ensure your suppliers understand and comply with your security policies.

3. **Implement a cybersecurity culture**

   A defence-in-depth approach is essential to protect your full digital ecosystem. This will require the support of the entire organisation. There are a number of ways to gain buy-in. Firstly, cybersecurity must be framed as a business issue. Leaders must work with other stakeholders to ask questions about the bottom-line and the reputational impact of a cyber threat.

   Look beyond your own boundaries and consider your supply chain and your customers – their safety is your safety. Adapt an always-on, "secure-by-design" mindset and address security proactively during the development and roll-out of new processes and technologies, as opposed to a reactive, costly afterthought.

4. **Detect and respond in real-time**

   Whilst the focus is on digital transformation, organisations must remember to ramp up their detect-and-respond

strategy to be able to counterattack breaches and threats in real time. Cybersecurity, IT/OT and business leaders must monitor threats 24/7 to anticipate and reduce their impact.

Organisations must look to adopt tools such as Security Incident and Event Management Systems (SIEMs) to monitor threats in real-time. As organisations pivot to the Internet of Things (IoT) and increase the number of connected devices in their networks, they should consider including anomaly detection technology to flag anomalous behaviour. Rapid response plans will help limit the damage caused by a cyber-attack and help protect your people.

5. **Recover and Share Lessons Learned**

An incident will occur, and leaders must learn as much from the incident as possible to ensure it is not repeated. Put together a recovery plan that will include processes to eliminate the cause of the breach, minimise its impact, and outline steps the organisation must take to get back up and running as safely, securely, and quickly as possible.

One of our biggest learnings is the need to have everyone in the organisation both aware of threats and what they need to do about them. Given that about 90% of malware is still delivered by email, do your people know handle to handle online risks?

6. **Secure your Digital Transformation**

Today, nearly every industrial firm worldwide wants to use digital technologies to improve efficiencies and reduce costs. They are incorporating smart devices that are connected to the internet. This digital transformation journey will need a new approach to cybersecurity. Organisations will need to rethink their approach to operational technology, with consistent and holistic security updates across devices.

Cybersecurity will always be a challenge for organisations, and it will become increasingly more difficult as digital transformation accelerates and cyber criminals attempt to exploit weaknesses and actively target the growing networks of connected devices. Prioritise developing your cybersecurity strategy and start acting now, to help mitigate your digital risk.

ABOUT QUINTIN MCCUTCHEON

Software Business Lead at Schneider Electric
▪ Secure your digital transformation journey with these six tips - 23 Sep 2020

View my profile and articles...