JOHANNESBURG, SOUTH AFRICA, 12 April 2022

**Why it is critical to have a robust cyber security strategy in place**

**By Charles Blackbeard, Business Development Manager, ABB Ability™ Digital Solutions**

The need for a solid cyber security strategy is constantly discussed and debated. Yet the basic worm-type attacks first documented in 1972 are still with us today. This is because even the most basic measures to protect control systems from these types of attacks are still not systematically employed. It is difficult to believe there are still thousands of systems in operation today without any basic security controls in place.

If you own a car, a house, or a boat — just about any ‘big ticket’ item that would be expensive to replace — you protect that asset with insurance. However, when it comes to control system cyber security, this thinking is often not applied. Cyber experts are still struggling to convince senior management to spend money to protect their control system assets.

Why do companies not invest in cyber security? Partly, it is due to the issue of convincing companies to spend money on something that has no measurable return on investment (ROI). Of course, everyone knows cyber security is important and falls into the general category of risk management.

Control system owners do deploy cyber and security solutions as they are aware of the problem and take actions to avoid risks. However, many in the industrial world are still too focused on the big attack or hack, when the more likely risk is common malware that impacts a control system because it is running older, unprotected, and unpatched operating systems.

This risk exists even if the system is ‘air-gapped’ from the business’s network. People often introduce data and software from removable media such as USB drives, exposing their systems to the potential for viruses along the way. As these air-gapped systems become more interconnected to enable integration with business applications, they become increasingly exposed to the internet.

This vulnerability occurs because there is a fundamental disconnect in securing operational technology (OT) versus information technology (IT). As OT becomes more exposed to the internet, it faces the same cyber security threats as any other networked system. As operators have adopted the same hardware, software, networking protocols and operating systems that run and connect everyday business technologies, such as servers, PCs, and networking equipment.

**Getting up to cyber speed**

When thinking about how to get started to fortify your Cyber Security profile, do not just look for some new technology that claims to mitigate all your risks — it does not exist. Doing the basics well before investing in advanced cyber technologies is the key. In order to minimise your risks and get the most protection in the least time, you first need to plan and develop a cyber security program that:

1. Identifies what assets you are trying to protect
2. Determines how you are going to protect those assets
3. Enables intrusion detection and monitoring
4. Defines incident response processes and procedures
5. Verifies mechanisms to restore and recover assets
6. Ensures compliance with all regulatory standards set by local governing bodies

These six steps follow well-trodden ground. All cyber security best practices frameworks can be distilled into these basic steps: identify, protect, detect, respond, recover, and comply. Understanding and managing the risks associated with a cyber attack and then protecting against these or mitigating the consequences can seem a daunting prospect, especially when this needs to be done in conjunction with the day job of keep a plant up and running.

ABB has enjoyed the following global successes in terms of its cyber security systems and solutions:

* For a specialty chemicals company in the UK, ABB provided training to help employees spot, understand, and remediate cyber security attacks. This was because the client had already identified a weakness in their employees’ knowledge regarding cyber security. ABB provided a Cyber Security Gap Assessment and recommended its T153 Cyber Security Training Course. The end result was increased awareness on the part of employees, reducing the likelihood of cyber attacks succeeding due to human error.
* For a natural gas storage facility in Germany, ABB provided a cyber security solution for regulatory compliance with ISO 27001. This was necessary for visibility of security events in DCS systems and connected networks and to allow continuity with a dedicated partner. ABB Ability™ Cyber Security Event Monitoring allowed for automated ISO 27001 reports and monitoring through ABB’s Collaborative Operation Centre in Germany.
* ABB also assisted a European energy provider with ISO 27001 regulatory compliance. ABB Ability™ Cyber Security Event Monitoring was implemented without affecting production. This robust solution was deployed across multiple IT and OT systems distributed over Austria. Here ABB’s OT security expertise also covered third-party vendor systems. Benefits included reduced effort to meet compliance deadlines, increased cyber resilience and access to ABB’s industrial cyber security experts.

Understanding and managing the risks associated with a cyber attack and then protecting against these or mitigating the consequences can seem a daunting prospect, especially when this needs to be done in conjunction with keeping a plant up and running. The old adage of it’s a journey not a destination is very true when it comes to OT cyber security. ABB can support companies with this journey, and can do so in small ‘bite-sized’ steps to help companies take the next step.

**ENDS**

**ABB** (ABBN: SIX Swiss Ex) is a leading global technology company that energizes the transformation of society and industry to achieve a more productive, sustainable future. By connecting software to its electrification, robotics, automation and motion portfolio, ABB pushes the boundaries of technology to drive performance to new levels. With a history of excellence stretching back more than 130 years, ABB’s success is driven by about 105,000 talented employees in over 100 countries. www.abb.com

|  |
| --- |
|  |

**For more information please contact:**

**Media Relations** **Issued by NGAGE Marketing on behalf of ABB**

Ofentse Dijoe Nomvelo Buthelezi

Phone: +27 (0) 010 202 5105 +27 (0)11 867 7763

Email: [Ofentse.dijoe@za.abb.com](mailto:Ofentse.dijoe@za.abb.com) [nomvelo@ngage.co.za](mailto:nomvelo@ngage.co.za)