Because They Have To Work

Considering Cybersecurity for Digital Enablers

Authors: Johannes Mäder, Martin Schade, Nicklas Söhner

1

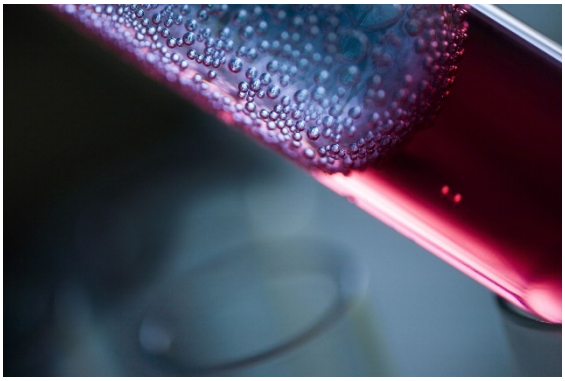
Digitalization Needs to Rely on Sound Enablers

In 2020, business is digital. In a speed that can only be described as breathtaking, we are labeling direct, personal contact as risky. Something odd and careless from the past, much like the extent of smoking in a 1950s motion picture. But at the same time, life must go on. Business must go on if we are to preserve our prosperity. And for now, digital is the only way things can "go on". Digitization has moved into the core of our daily lives like a visionary digital evangelists' keynote come true. Everyday products? Home appliances? Food? Now have a broad smile on the cardboard boxes they arrive in. When did you last eat out? When was the last party you attended? And while researchers have yet to find out how this is changing society, one is clear already: If digital infrastructure was important in 2019, it is essential in 2020 and beyond. If digital business was contributing majorly to a company's success last season, it is now what stands between future and bankruptcy, at least for many businesses.

Enablers Are Business-Critical and Should be Safeguarded as Such

Digital infrastructure, be it IoT, cloud or data transmission, have become the lifeline of many businesses. Digital enablers make new and adopted business models possible. If set up smartly, they may even enable scalability. But should the enabling fail, the effects may result in a temporary loss of market access, reputation, or even operational safety. As always when assessing risk, if the potential impact is devastating, the likelihood of occurrence shall be minimized. Therefore, digital enablers should be protected by design. Cybersecurity must be integrated through the whole digital enterprise. From the early use case design up to a sundown, cybersecurity must be embedded into the digital infrastructure to be effective. The following two examples have been chosen to picture the close interdependence of cybersecurity and digital infrastructure.

Out of Day-to-Day Operations



Example 1: IoT monitors blood plasma status

Blood transfusions are used for important healthcare services. This entire life-saving system relies on the altruism of contributors. For example, in the US blood that is transfused into a patient must be donated. It cannot be bought or produced which highly limits the supply of blood.

Around 20% of temperature-sensitive biopharmaceutical products are damaged during cold chain transport. Tracking and monitoring sensors provide real-time visibility into temperature changes and an opportunity to intervene before damage is done. Who has handled the goods? Has the cargo deviated from its

planned route? Have container or package been opened prior to arrival? These types of asset visibility measures safeguard both the physical security and quality of the cargo.

However, this also introduces unique risks which are adding onto the risks of traditional IT systems. The security provided for such a critical asset must be appropriate for what its worth. All information the system provides is worth nothing if the integrity, confidentiality, and availability of the data cannot be assured. To build models relying on a continuous stream of information from the field, the channel as well as the platform must be holistically secured.

Spanning from the product being engineered to data being used, it needs to be protected against manipulation. This can be achieved by applying a set of standard tools. The first step should be to create a system to monitor and safeguard data integrity, a root of trust. As next step, a reliable encrypted connection for assured real-time transfer of sensible data should be established. Data then is stored on a highly access-controlled platform for data collection and usage.

Each of these steps to implement cybersecurity should follow a concise strategy. Moreover, it should be professionally managed and integrated into the organization.

Example 2: Cloud data – how to share it with business partners?

Most of the value the cloud generates comes from increased agility and innovations. It can be obtained by following a holistic strategy. This strategy should encompass standardization and automation of IT environment through an open API model. Also, it should leverage new capabilities to drive innovative solutions which are complimentary to today's core business model.

This strategy can be best implemented by platforms, on which data sharing with business partners takes place in a standardized manner. Furthermore, constraints in the form of cost and risk in fields such as technology, sourcing and data migration can be addressed. To launch these platforms and multiply both data and value potential, there will be a need of a close collaboration between a multitude of players.

Further collaboration always introduces increased complexity. And the security need of a cloud environment scales with its complexity. From handling different data security standards, to complex identity and access management solutions the collaborative nature of digital enablers and the cloud will drastically increase the efforts to be invested into security. Following a planned scaling of cybersecurity activities might grant the deciding edge over the conventional organic growth of activities.

Nevertheless, the value of clouds by far surpasses the cost of a well thought-through and integrated cybersecurity approach.

3

Ginkgo Can Assist You in Enabling Your Business Securely

Digitalization is now more important than ever; digital enablers are the basis for sustainable business. Considering cybersecurity in design and interaction with said enablers can greatly increase resilience of businesses, as the examples have shown. Both aspects, business / IT on one hand and cybersecurity on the other, should be considered as part of the same picture. Understanding both is essential to success, to getting digital done securely.

4

About the Authors

Johannes Mäder - Manager

Johannes focusses on the design and set up of IoT systems in several industries. With his background as industrial engineer, he also advises clients on the implementation of use cases based on IoT data.

Martin Schade - Manager

Martin focusses on digital transformation projects in several industries to help clients develop sustainable competitive advantages through IoT, Connectivity, Cloud and Big Data.

Nicklas Söhner - Senior Cybersecurity Consultant

Nicklas is experienced in the field of cybersecurity for IT and IoT systems. He supports his clients in the automotive and smart-home industry from the concept to the technical implementation.