A Challenge for IT Security Experts: Small and Medium Enterprises and Industry 4.0

By Goodarz Mahbobi

Goodarz Mahbobi, CEO at the IT and management consultancy axxessio GmbH in Bonn and Darmstadt

Digitization is moving forward at a rapid pace – it affects society and economy, countries and cities, as well as large companies and small and midsize enterprises. Bigger players usually have enough resources to deal with the consequences of the digital transformation; however, for smaller players often-times this is not the case. Moreover, they need to use their limited resources to adapt even more fundamentally.

In 2015, Ashok-Alexander Sridharan, Lord Mayor of Bonn, and I started the initiative "Digital Bonn" to motivate involved parties in government and business in the region to take on a more strategic approach to digital transformation. One of the first plans implemented was the foundation of the "Cyber Security Cluster Bonn" for the Bonn/Rhein-Sieg region to set up an "army of the good." This has been a major milestone for the initiative due to IT security's critical role in new digital processes. Although IT security is a base requirement, even the IT industry itself still has some large blind spots in this area. So do cities and SMEs – but they cannot simply deal with this by spending large amounts of money. They need a different approach.

To gain a better understanding of the situation, we took a closer look at the state of IT security in Germany's industrial SMEs. German SMEs are extremely successful; still, the digitization of the industrial sector and the improvement of IT security present a major challenge to them. To overcome this potential disruption and keep its status as one of the leading industrial nations, Germany has developed an "Industry 4.0" strategy. Industry 4.0 requires the integration of digitalized assets with communication networks – hence, IT security becomes a critical factor for its success.

While the perceived importance of IT security among SMEs is generally high and increases with company size, there still is a great discrepancy between perception and action. This is indicated by the small pro-portion of SMEs that have actually carried out an IT security analysis.[1]

This lack of action can be linked to SMEs' lack of empowerment regarding IT security, which has been confirmed by various surveys. In summary, SMEs would like to understand the IT security problem better – but there is a need for better information; trustworthy external IT-security consulting; training; better, more user-friendly security software; and standardized IT security measures.[1]

1 A. Hillebrand, A. Niederprüm, S. Schäfer, S. Thiele, und I. Henseler-Unger, „Aktuelle Lage der IT-Sicherheit in KMU". WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, 2017.

Missing this kind of support, decision-makers in SMEs do not ignore the problem but turn to sources of information they trust. In Germany, they primarily rely on their social network of other companies to search for information, exchange ideas, and discuss problems in closed forums.[2] However, by relying on familiar social networks and not turning to new sources of information, the situation stagnates and IT security awareness cannot be improved. This was particularly evident in the development of planned investments in IT security between 2011 and 2017: more companies invested in IT security, but the overall level of investment did not increase. Above all, the biggest problem is the 54 percent of companies that either have no investments planned or answered "they don't know" in response to a question about whether they are planning new investments.[1]

The question remains regarding what measures could increase the investment in IT security among SMEs at this point in time. Surveys show that for SMEs, the greatest influence on investment in IT security is exerted by regulatory requirements, digital transformation, and customer requirements. Regulatory re-quirements are powerful since they affect all competitors equally. Digital transformation investments always come along with IT security investments since these form an important basis for digitization. Fi-nally, customers can exert great pressure on SMEs to meet their requirements, which are at this time often linked to Industry 4.0 projects. Other incentives for IT security investments are strategic business orientation, industry standards, and recent media coverage of cyberattacks. Surprisingly, surveys found that current security incidents in one's own company or within an industry have the smallest impact, compared to the aforementioned reasons.[3]

Industry 4.0 can play a significant role in IT security awareness: 76 percent of managers expect an increased IT security risk to accompany Industry 4.0 investments.[2] Therefore, companies active in the In-dustry 4.0 sector attribute greater importance to IT security and more frequently perform IT security analyses. They are forced to deal intensively with their processes and data, which leads to a better understanding of their assets. Moreover, they assign higher significance to their assets and data protection. This is reflected in the survey results of "Industry 4.0 companies" compared to companies not active in the field of Industry 4.0: the need for data protection for R&D data doubled, rose about 8 percent for process data, and increased by 15 percent for machine data.[1]

Clearly, Industry 4.0 has a positive impact on SMEs' IT security activities. At the same time, however, data protection and data security requirements are still seen as the biggest barriers for the implementa-tion of Industry 4.0 itself.[4] The development of Industry 4.0 and IT security are heavily interdependent; they can boost or inhibit each other.

Oftentimes IT security is not taken into account right from the start. Subsequent changes are always expensive and sometimes impossible. Still, we have seen that overall interest to invest in existing pro-jects is low – new, well-planned IT projects, especially in the field of Industry 4.0, can boost the motiva-tion to take IT security seriously. Furthermore, the IT security sector can support SMEs' efforts in Indus-try 4.0 by better understanding the requirements they are trying to fulfill. These are often a result of market competition: 60 percent of surveyed companies responded to be in a cost and quality competition and 31 percent to be in a time and innovation competition.[5] It is of crucial importance that the IT security industry adapts its offers to the needs, the competitive situation, and the IT security obstacles of SMEs. Only in this way can SMEs keep up with development.

2 „Cyber Security Report 2018 Teil 2: Unternehmen – das Risikobewusstsein sinkt". Deloitte, 2018.
3 P. Engemann, D. Fischer, B. Gosdzik, T. Koller, und N. Moore, „Im Visier der Cyber-Gangster So gefährdet ist die Informationssicherheit im deutschen Mittelstand". PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC), 2017.
4 A. Berg, „Industrie 4.0 – Wo steht Deutschland?" bitkom, 2018.
5 „Industrie 4.0 im Mittelstand". Deloitte, 2016.