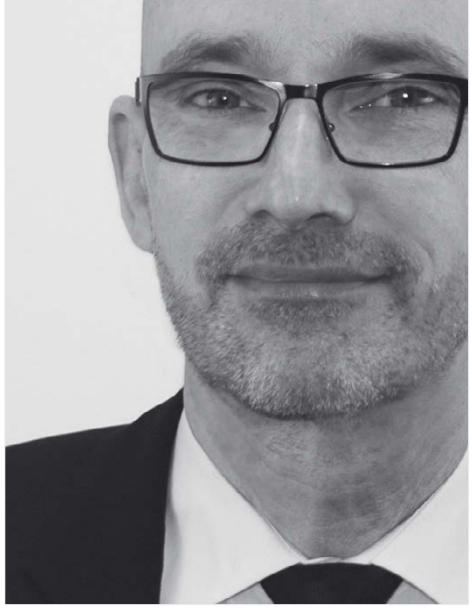
Editorial

Cyber Security and Compliance

Manfred Tubach



Manfred Tubach
CEO
usd AG, Neu-Isenburg

When it comes to everyday life, we instinctively recognize danger. People are alarmed and, for example, subconsciously start to walk faster. In the digital world, however, our senses and reflexes fail. Recognizing and defending threats in this digital environment requires awareness, knowledge, and effort.

Experts have long been warning us of ever new and increasingly dramatic threats under the catchphrase of "cyber security". A vast number of articles, standards, and laws address this topic. Depending on their intent, the various authors worry about public welfare, vital infrastructure, specific data, individual sectors, and – nine times out of ten – small and medium-sized enterprises. Security experts very often find such recommendations and regulations too vague and thus of little help. What are, for example, "appropriate state-of-the-art security measures" as required in contracts or insurance terms and conditions?

Managers with no expertise in IT have always had trouble making decisions in this field. It is even more difficult for them to decide about complex IT security measures, as costs are high and benefits vague. Imagine your company urgently needs a new corporate mobile app. Features, dates, and budgets are clear, security is of course requested but remains hazy regarding its contents. Which items will be cut when things get tight? Functionality? The cool design? Or the security concepts, vulnerability analyses, and security audits?

The payment card industry, which has been an attractive target for criminals for many years, solved these questions by creating the Payment Card Industry Data Security Standard or PCI DSS for short. All payment card organizations, be it VISA, MasterCard, American Express, CUP or Diners, require compliance with this standard which is defined and continuously updated by a central council. Any company worldwide that comes into contact with payment card data has to be PCI DSS compliant. The standard precisely defines who has to do what, depending on size, role, and risk. The requirements, that amount to well in excess of 200 at the top end, concern technical, organizational, and awareness issues for employees. Security analyses and certifications may only be conducted by accredited and certified auditors whose suitability and results are continuously monitored. Companies that are PCI DSS compliant benefit from safe harbor rules, all the others pay risk premiums, bear existential risks, or are excluded from the market.

As a PCI Qualified Security Assessor, we provide consulting services to and certify thousands of companies world-wide, including online stores, large merchants, payment service providers, processors, and acquirers. Even though we make every effort to support our customers, it is still challenging for them to sustainably fulfill the required actions. It is very helpful that the wording of the requirements is relatively practical and precise thus making decisions easier and improving the quality of solutions and services. As a result, companies don't only become "PCI DSS compliant", they also reduce their risks through increased security.

Many security managers who want to improve IT security or have to comply with only a few precise security requirements adapt the concepts, tools, processes, and trainings of the PCI environment. This enables them initially to save time and money. However, we find that it is more important that management, customers, and business partners intuitively understand and appreciate the message: "In the field of cyber security, we are aligned with the requirements of the payment card industry."