Cybersecurity Trends 2019, a report that contains eight important developments in cybersecurity.

TREND 1: Cybersecurity has become a topic for the management level
Until recently, lack of cybersecurity was not seen as a business risk, but as an IT problem. Despite years of warnings, it was only the effects of the NotPetya cyberattack in 2017 that changed this view. Several large companies reported losses as a result of this attack, including logistics companies Maersk and FedEx, advertising company WPP and household goods manufacturer Reckitt Benckiser. These companies have reportedly each lost up to hundreds of millions of euros. At the same time, breaches of data protection remain a cause for concern. Risks associated with a lack of cybersecurity have evolved from a hypothetical problem to a recognized business risk. This realization is now leading to long-term changes in the management of cybersecurity risks.

TREND 2: Industrial cybersecurity is years behind general IT security
In an Operational Technology (OT) system, computers recognize or modify physical processes by controlling and monitoring devices such as electric motors, valves or relays. Although the lack of cybersecurity of OT systems can have serious consequences, industrial cybersecurity has long been neglected and has been characterized by both indifference and underinvestment. Today, the risks of neglecting the protection of OT systems have fundamentally changed due to new technologies and geopolitical tensions.

TREND 3: Standards pose a challenge for IoT cybersecurity
Standards organizations and industries around the world are developing the security and privacy standards needed to secure the next stage of development in the Internet of Things (IoT) and Operational Technology (OT). Although well intentioned, it can be confusing and time consuming for manufacturers to find out which of these regional and industry standards they need to consider. Particularly affected are global companies that need to understand how to ensure compliance when developing their products. The existence of competing standards could therefore lead to a waste of time.

TREND 4: The pressure caused by the GDPR represents a turning point for consumer data protection
The European Union (EU) General Data Protection Regulation (GDPR), enforced as of May 2018, held many unknowns. Although overall enforcement is relatively slow to start and the first fines imposed were rather low, it is clear that the DSGVO will have a significant impact on data protection not only in the EU, but worldwide. For most industries, it will simply be cheaper to develop and design their products and services to meet the highest global standards, rather than limit themselves to geographically limited privacy.

TREND 5: The shortage of skilled workers in cybersecurity will distort the labor market
While the importance of cybersecurity has increased, the staff needed to meet the specific cybersecurity demands have not. It is estimated that by 2020, there could be a shortage of 1.5 million skilled workers worldwide. An extreme shortage of skilled workers often leads to market distortions: Larger, financially stable organizations and service providers are able to recruit competent staff, while smaller companies may have problems in some sectors. Inevitably, this

not only makes cybersecurity more expensive, but also affects supply chains that connect large and small businesses, economically. In terms of the long-term interests of the industrial economy, cybersecurity is of importance to the general public and should be accessible to all.

TREND 6: The detection and response to threats depends on the establishment of Security Orchestration, Automation and Response (SOAR).
The security orchestration, automation and response (SOAR) approach reduces the time required to detect incidents, accelerates threat response and minimizes the impact of cyberattacks. The greatest added value is provided by automated threat containment workflows, which are critical in dealing with rapidly spreading malicious malware. Other benefits of SOAR include standardization of cyberattack investigation processes, faster prioritization and response, the ability to proactively search for threats and improved quality and efficiency of detection and response processes. However, to implement a new wave of automation with SOAR, organizations must invest and plan at a time when established investments such as Security Information & Event Management (SIEM) solutions are just beginning to pay off.

TREND 7: "Red Team" tests and agile security gain general acceptance
The terms "Red Team" test and "holistic test" have their origin in the field of penetration testing. "Red Teams" simulate how an attacker can penetrate an organization and gain access to resources under real-world conditions by exploiting existing vulnerabilities. While vulnerabilities can be found in many resources (applications, devices or infrastructures), "Red Teams" also simulate topics such as social engineering, hijacking social media, physical access to a building or - in extreme cases - their own employees with malicious intentions. Unlike traditional pen testing, Red Teaming tries to understand how these factors interact and does not look at them separately.

TREND 8: Cybersecurity decides on winners and losers of the digital economy
The modern world is rapidly developing into a digital, knowledge-based "industry 4.0" economy. This change has a similar meaning as the industrial revolution in the 18th century. A fundamental challenge in this process is to recognize how to ensure one's own security, where the resources should come from and what global standards are needed to make development as smooth as possible. The ability to meet the security challenges of the digital economy will determine the success of economies, economic sectors and perhaps even the political systems on which they are built. It is possible that for many large organizations this will result in a simple scenario of either success or failure without a middle course.