Charter of Trust

SIEMENS
Ingenuity for life

Munich Security Conference

Charter of Trust on Cybersecurity

Cybersecurity – one of the most important issues today

The most important decision-makers in international security policy will be gathering once again at the Munich Security Conference (MSC) from February 16 to 18, 2018. Some 500 VIPs from all over the world will meet to discuss current crises and future challenges in international security policy. As a strategic partner of the MSC, Siemens will be making the most of the occasion to highlight a topic that's not just extremely relevant to companies, but also poses major challenges for the entire world: cybersecurity.

Threats to cybersecurity are estimated to have caused above €500 billion in damage in 2017 alone. For certain European countries, the damage amounts to 1.6 percent of their GDP. And the scope of cybersecurity threats is growing: 8.4 billion connected devices were in use in 2017 – 31 percent more than in 2016. This number is projected to reach 20.4 billion by 2020.

Adequate cybersecurity is one of the basic requirements for protecting critical infrastructures and sensitive data as well as for maintaining uninterrupted business operations. This means that cybersecurity is more than just a metaphorical safety-belt: It's a critical factor in the success of the digital economy.

People, organizations, and even entire societies all over the world need to rely on trustworthy digital technologies. Yet, we can't expect people to actively support the digital transformation if it cannot be ensured that their data and networked systems are adequately protected according to the current state-of-the-art. That's why digitalization and cybersecurity are two sides of the same coin and must evolve in parallel. If either one is to work properly, they both have to function seamlessly. That's especially true in an era when digitalization is moving into every area of life. Defects or even outages in the systems that control and network our homes, our hospitals, our factories, our power grids – in fact our entire infrastructure – could have appalling consequences. Modern regulations, protected environments, and clear standards for cybersecurity are an essential prerequisite for people to trust our digitalized world – and it's essential to earn that trust, because it's the linchpin for the future success and prosperity of us all.

That's why Siemens' CEO Joe Kaeser announced in November 2017 that – at the Munich Security Conference – Siemens will create and sign with partners from industry, government, and society a "Charter of Trust," and will make this charter public, and push for its general adoption. The charter advocates ten principles intended to make our digital world more secure, and it's aimed at three important objectives:

- Protecting the data of individuals and companies,
- Averting harm from people, companies and infrastructures, and
- Establishing a reliable basis where confidence in a networked, digital world can take root and grow.

And it describes what it will take to achieve these goals: First of all, hedging the all-encompassing impact cybercrime and creating a common basis of trust across globalized markets requires strong multilateral collaboration between politics and business. Responsibility must be taken at the highest levels of government and corporate entities and has to be reflected by clear targets and measures in the respective organizations. Moreover, accountability for cybersecurity needs to be ensured along the entire digital value chain. This encompasses fundamental and ongoing education and professional training in cybersecurity. Firms and policymakers should also – as described in the Charter – deepen their common understanding of cybersecurity requirements and ensure that modern rules and standards required to continuously develop and adapt technologies in the field of cybersecurity are established and adhered to. Data flows don't stop at national borders; that's why everybody profits from rules that are applied internationally.

No single entity can be tasked with implementing all of the necessary measures – not even a global player like Siemens. With our "Charter of Trust" we are attempting to initiate close collaboration on all levels. Information, product and solution security must be an integral part of our digital world. We are convinced that businesses and countries that want to play leading roles in the global digital markets will have to jointly engage in cybersecurity to sustain the trust of societies, customers and business partners.

Further information

charter-of-trust.com
siemens.com/cybersecurity
siemens.com/pof-cybersecurity

Cybersecurity – an important pillar of Siemens' digitalization strategy

Cybersecurity is a top priority for Siemens. The ability to supply customers with products and systems that contain state-of-the-art cybersecurity functionalities is a competitive advantage in the growing digitalized business world. A McKinsey study based on 250 interviews with industry leaders states: "Major technology trends like massive analytics, cloud computing and big data could create between US$ 9.6 trillion and US$ 21.6 trillion in value for the global economy. If attacker sophistication outpaces defender capabilities – resulting in more destructive attacks – this could slow innovation, with an aggregate economic impact of around US$ 3 trillion."

The cybersecurity business is expanding dramatically, for both products and services. Analysts estimate that the security market for industrial controllers will grow at a rate of seven percent from US$ 9 billion in 2016 to US$ 12.6 billion in 2021. At the same time, there's a growing demand from customers for cybersecurity services: for example, to safeguard entire infrastructures like factories and power grids against cyber-attacks.

With its unique combination of technical expertise in cybersecurity and extremely deep domain knowledge, Siemens is ideally positioned to be both a market and a thought leader. Currently, our company has about 1275 cybersecurity experts worldwide, which includes about 25 white-hat hackers who continuously challenge the security of both internal IT systems and products being shipped to customers. And cybersecurity is far from a new topic at Siemens: The first IT Security team at Siemens was established in 1986 – about 30 years ago – at the company's central research department, Corporate Technology.

With more than one million devices already connected to MindSphere, we have first-hand experience with cybersecurity challenges in the age of the Industrial Internet of Things.

Siemens is the first company to have – in its Digital Factory Division – security integrated in all phases of its industrial product development lifecycle and to be certified by TÜV Süd for this purpose. Specifically, Siemens offers Plant Security Services, which include assessing security risks in factories and production plants as well as implementing security measures for our customers based on IEC62443 and the Holistic Security Concept. The latter may include implementing antivirus software, security trainings, firewall management, antivirus management, and incident handling.

Siemens also offers cybersecurity services for industrial customers, utilities and power grid operators as well as for healthcare providers, including the evaluation and continuous monitoring of the current system, implementation, testing, and maintenance of security upgrades, and response to cyber incidents.

Some examples of our research also reflect the company's leading position in this field. Siemens is providing tested and hardened components, developing automated intrusion detection and response in the industrial context, and automating "security along the lifecycle" concepts for industrial equipment. Cybersecurity is one of our top core technologies and research areas.

Siemens is a member of FIRST, the umbrella organization for all CERTS (Cyber Emergency Response Teams). We also have a very good relationship with national CERTS (such as US-CERT, EU-CERT, and ICS-CERT) and law enforcement agencies (like the FBI, BKA, Europol, and DHS), and we gather threat intelligence and share them via these alliances. We've formed partnerships for developing industrial IT and standards and collaborations with universities, business partners, customers, startups, and respected research institutes on cybersecurity innovations.

In short: With its unique and diverse industry expertise and comprehensive cybersecurity technology solutions, Siemens is a reliable and preferred partner for customers who aim to achieve a superior level of cybersecurity for their systems – from factories to power grids and healthcare.

Contact for journalists

Florian Martini

phone: +49 89 636 33446;
e-mail: florian.martini@siemens.com

Follow us on Twitter: www.twitter.com/siemens_press