SIEMENS

Ingenuity for life

Cybersecurity Backgrounder

Cybersecurity for Critical Infrastructure Protection

siemens.ca/cybersecurity

Digitalization and globalization are shifting paradigms and bringing new opportunities. Billions of devices are connected by the Internet of Things, interacting on an entirely new level. These technologies are changing the way we live, communicate and work. They are enabling new applications and business models across all industrial sectors and verticals. Artificial intelligence, big data analytics, blockchain and cloud technologies are improving our world in countless ways.

But these new connections bring new vulnerabilities. They also increase our risk of exposure to malicious cyberattacks. The world has experienced how such attacks can influence democratic elections. More and more, critical infrastructures such as banks, government, industry and health services are also targets. Close to $600 billion USD, nearly one percent of global GDP, is lost to cybercrime annually.[1]

Hackers aren't just attacking conventional PCs. Ever since the Stuxnet malware made headlines worldwide in 2010, manufacturing companies have realized that advancing levels of digitalization are blurring the lines between offices and the infrastructures that control industrial facilities. As a result, plant operators have had to prepare for all the challenges that the Information Technology (IT) sector is familiar with – the global WannaCry cyberattack confirmed this in May 2017. With more and more products, solutions and services employing software used in critical infrastructure, the range of cybersecurity risks will continue to grow. As a result, more than eight billion devices, including machines, facilities, sensors, and products, now communicate with one another, representing an increase of about 30 per cent since 2016. This number will continue to climb dramatically – to more than 20 billion by 2020.[2]

Although there has been progress on the well-known cybersecurity for IT, there is much work to be done for critical infrastructure cybersecurity, known as cybersecurity for Operational Technology (OT).

The message is clear. Failing to protect the systems that connect and control our homes, hospitals, factories, power grids and infrastructures could have devastating consequences. The digital world needs baseline security, to match the commonly accepted safety measures we take for granted in the non-digital world. Fostering trust in cybersecurity requires a broad alliance of companies and governments to act. No single entity can do it. Decisions must be taken now.

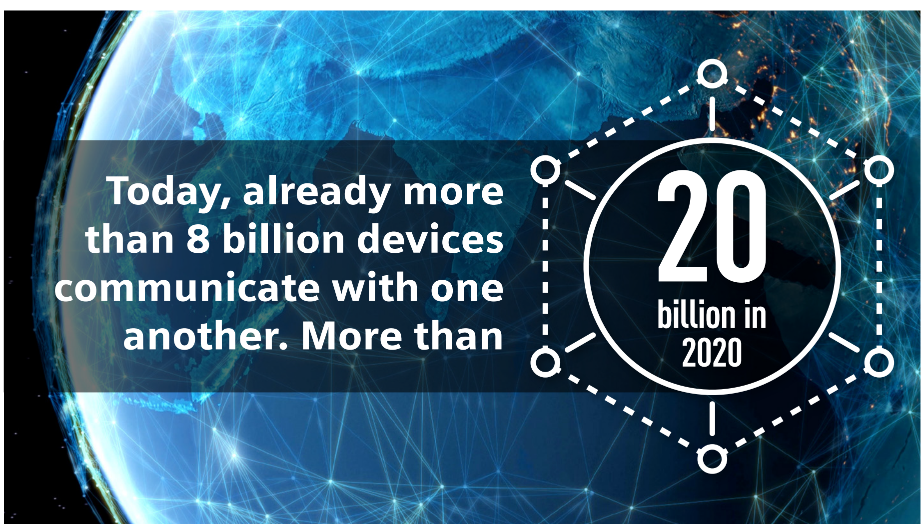
As an initiator of the Charter of Trust, Siemens is taking the issue of cybersecurity to a new level. Together with several other large companies such as Daimler and IBM, the company has launched a powerful global initiative: The future products of all the partner companies will be designed and implemented according to ambitious cybersecurity principles.

Siemens employs cyber defense experts to examine industrial facilities worldwide for possible threats from the Internet, warns companies of security-related incidents, and coordinates proactive countermeasures. The company currently employs about 1,300 cybersecurity experts. This gives Siemens a very broad foundation for protecting itself and its customers with secure products and systems. Moreover, cybersecurity systems are among Siemens "Company Core Technologies" – i.e. technology and innovation areas that are of the greatest strategic significance.

As a result, the company has a substantial amount of expertise in the field of cybersecurity and the growing challenges it poses. This applies especially to MindSphere, Siemens operating system for the Internet of Things (IoT). Already today, more than 1.4 million devices from a variety of customers are now connected to this system. All of these devices have to be protected, especially as their numbers continue to increase. In addition to its focus on industrial customers, Siemens also provides cybersecurity services to suppliers, power grid operators, and the healthcare sector.

In Canada, in May 2018, Siemens established a global Cybersecurity Centre in Fredericton, New Brunswick with Opportunities New Brunswick. The centre is operational and will focus on research and development, consulting and managed services. The Siemens Cybersecurity Centre aims to bring together Siemens' expertise in critical infrastructure protection with New Brunswick's emerging cybersecurity ecosystem, creating potential for global exports of locally created internet protocol, methods and technology. The venture is expected to create up to 30 highly skilled jobs in the province by 2020 with another 30 jobs in Phase 2, and will also support training, education and research and development. The new positions are expected to be in engineering, research and consulting.

In 2019, Siemens continued its commitment to cybersecurity by joining the University of New Brunswick's Canadian Institute for Cybersecurity.



[1] 2018 Economic Impact of Cybercrime report by The Center for Strategic and International Studies (CSIS) https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

[2] Gartner press release, 2017. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

Siemens Canada Limited
1577 North Service Road East
Oakville, Ontario L6H0H6

siemens.ca/cybersecurity