

Cybersecurity: A major challenge

Critical Infrastructure Protection

Cyber/Physical Security

March 10th, 2021

Global Trends are driving our challenge



Growing
cyber risk to
businesses



Fundamental
technological
changes



Workforce
gap is
widening



Increasing
professional
hacking



More laws and
regulations
worldwide



Challenging
local vs. global
regulation

Adapted from source: Charter of Trust presentation, March 2021

Top 10 Challenges...

costs are expected to grow by 15 percent per year over the next five years, reaching \$10.5 trillion USD annually by 2025, up from \$3 trillion USD in 2015.

2019

1. Data Breaches
2. Skills Gap
3. Cloud Security
4. Automation & Integration
5. Awareness
6. Mobile Devices
7. State Sponsored attacks
8. IoT Devices
9. AI everywhere
10. Phishing

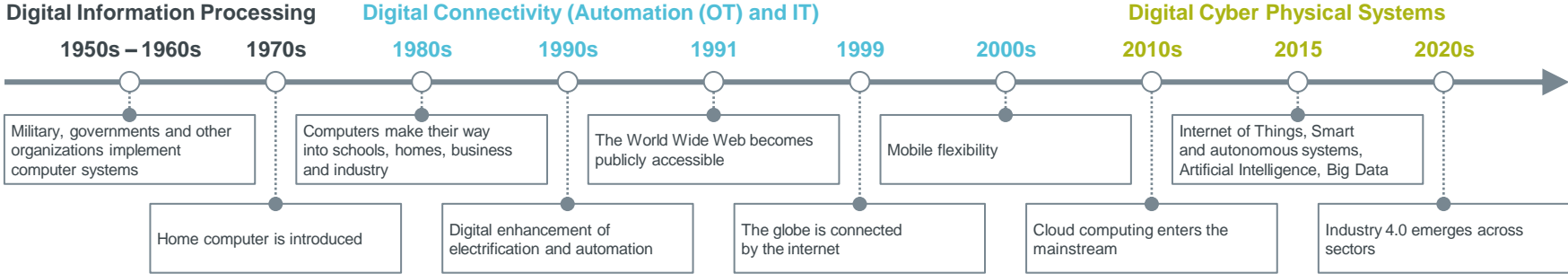
2020

1. Cloud Based Threats
2. Insider Threats
3. Remote Worker Endpoint Security
4. Phishing attacks
5. Deepfakes
6. IoT Attacks
7. Malvertising
8. Fileless Attacks
9. Ransomware Attacks
10. Social Media Based Attacks

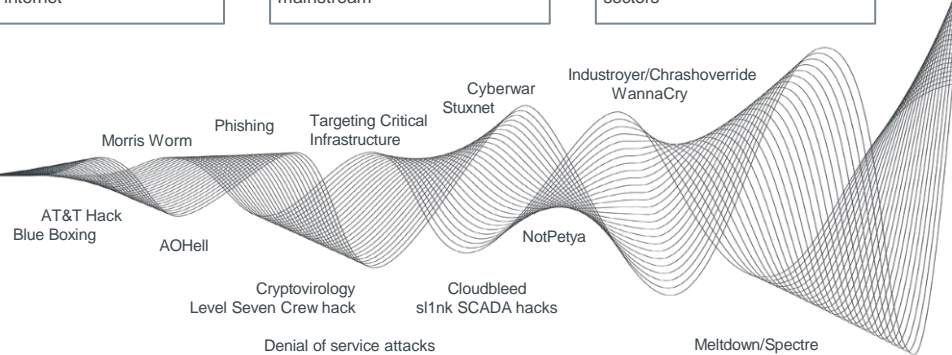
2021

1. Attacks on remote infrastructure
2. Autonomous Smart Devices
3. Internet as one large service factory
4. Centralized outage faults
5. Advanced non-nation state attacks
6. More bandwidth to secure
7. Bot Mitigation from Social
8. Ransomware
9. Fake News
10. Covid Propaganda

In a nutshell: As Energy and Industry digitalize... our cyber threats grow and evolve



The **threat landscape** keeps **growing** and **changing** and attackers are **targeting critical infrastructures** enabled by **Operations Technologies (OT)**



Our Value Proposition

We offer a comprehensive approach to secure heterogenous Operations Technology (OT) improving resiliency of Critical Infrastructure.

Energy assets need to be considered as a system from central operations to grid edge.

Key considerations are as follows:

- Security Management,
- Security Engineering,
- Security Operations,
- Security Testing and if required
- Security product/solution development

Our contribution: A Cyber Defense Centre in Fredericton, NB a part of Canada's security fabric

Cyber Centre
Phase One
@ Knowledge Park

A purpose-built facility specifically designed to be highly secure and highly resilient to protect both R&D and operations



Critical Infrastructure Services



Cyber Defense Centre



CYBERNB | CIPnet

Research & Development



Atos



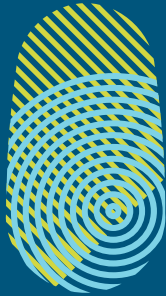
DAIMLER

DELL Technologies

SGS



TOTAL



Charter of Trust

charter-of-trust.de

SIEMENS



AIRBUS

Allianz



Munich Security Conference
Münchner Sicherheitskonferenz



Our Commitment

A joint initiative for a secure digital world

- 1 Protect the data of individuals and companies, ...

- 2 ... prevent damage to people, companies and infrastructures and ...

- 3 ... establish a reliable foundation on which confidence in a networked, digital world can take root and grow.

Within the framework of the Charter of Trust, the company has opened a **Global Center of Competence for Cybersecurity in Fredericton, New Brunswick**. This center is operational as of Fall 2018.

SIEMENS

| Contact

Published by Siemens Canada Limited

Richard Wunderlich

Strategic Development

Smart Infrastructure / Canada / Digital Grid

1577 North Service Road East

Oakville

Ontario

Mobile +1 (416) 294-5861

E-mail richard.wunderlich@siemens.com

Disclaimer

© Siemens 2021

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.