IoT in Education

Increasing Cyberattack Vector

An Evolving Cyber Threat Landscape

What it means to us?

MORE PHYSICAL SAFETY OF CANADIANS IS BEING PUT AT RISK

68% of manufacturers plan to increase their investment in IT-OT convergence solutions

MORE ECONOMIC VALUE IS BEING PUT AT RISK

An increasing number of Canadians have moved their financial activity online, thereby increasing their susceptibility and attractiveness to cybercriminals

MORE COLLECTED DATA INCREASES PRIVACY RISK

Canadians generate an incredible amount of data about their locations, shopping habits, patterns of life, and personal health when they use their phones and computers, bank and shop online, wear their smart watches and fitness trackers, arm their home security systems, or monitor their insulin levels with smart medical devices.

92% of Canadians expressed concern about the protection of their privacy, with 37% stating that they were extremely concerned

4 ADVANCED CYBER TOOLS AND SKILLS ACCESSIBLE TO MORE THREAT ACTORS

The commercial sale of cyber tools coupled with a global pool of talent has resulted in more threat actors and more sophisticated threat activity

5 INTERNET AT A CROSSROADS

Online foreign influence activities have become a new normal, and adversaries seek to influence domestic events like elections as well as impact international discourse related to current events.
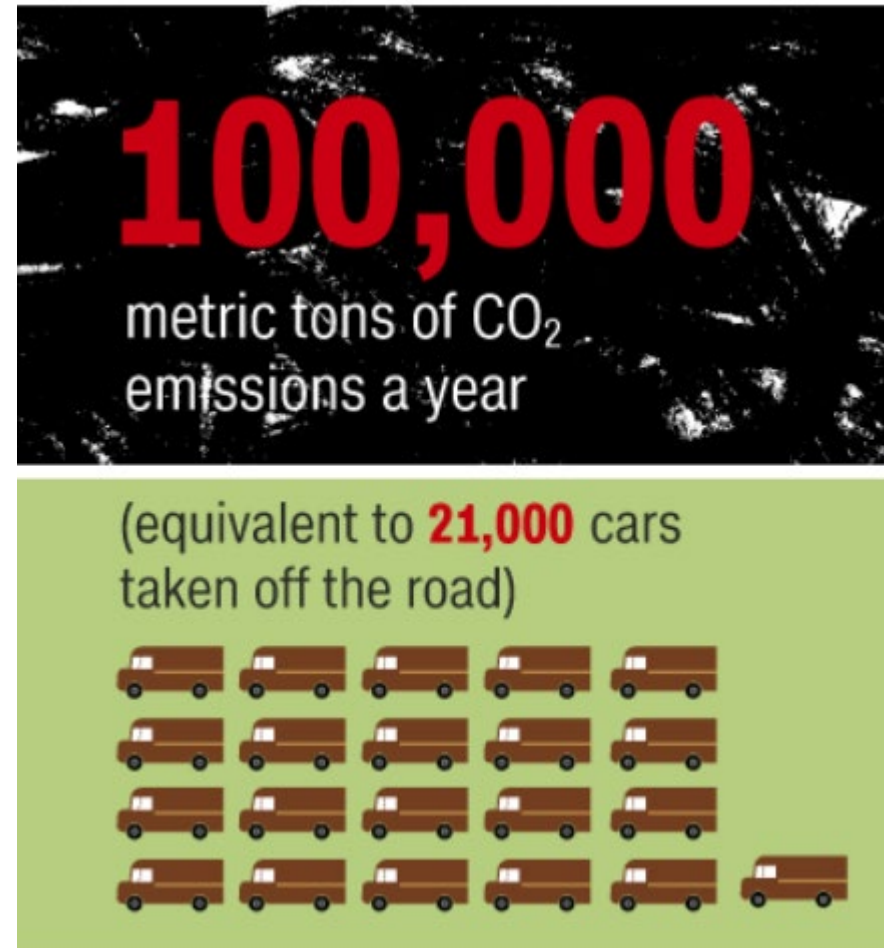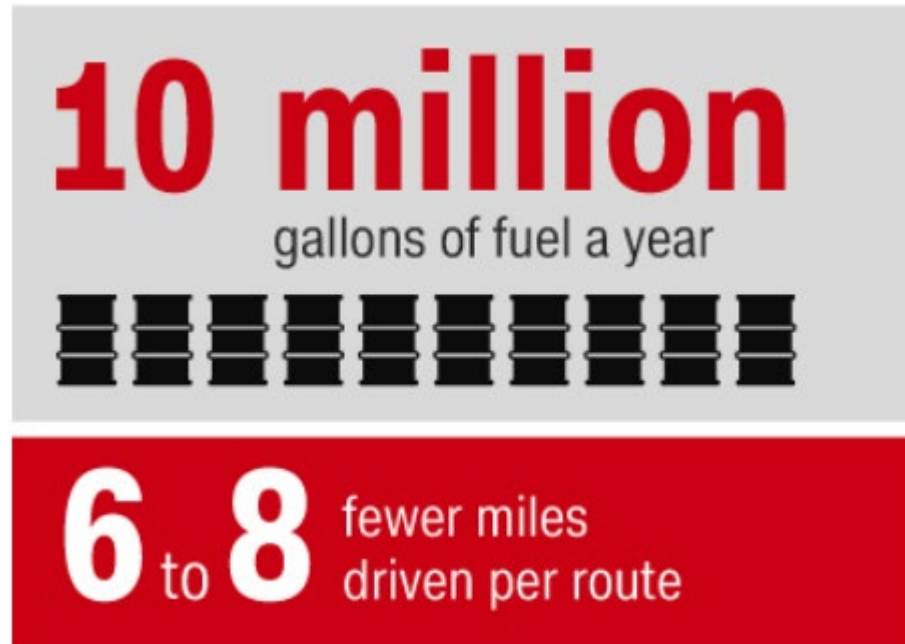
BCNET CONNECT

COMPUGEN
Dream. Design. Deliver.

Approaches to Security

"Canadians benefit greatly from living in one of the most Internet-connected nations in the world, and the cyber risks we identify in this report can be mitigated. *In fact, the vast majority of cyber incidents can be prevented by basic cyber security measures.*"

Sami Khoury
Head, Canadian Centre for Cyber Security

A 2016 Study !!!

10 million gallons of fuel a year

6 to 8 fewer miles driven per route

100,000 metric tons of CO$_2$ emissions a year

(equivalent to **21,000** cars taken off the road)

UPS

Cybersecurity is not only about Technology !

BCNET CONNECT

COMPUGEN
Dream. Design. Deliver.

Wholistic Approach to Cybersecurity

People

Process

Structured Approach
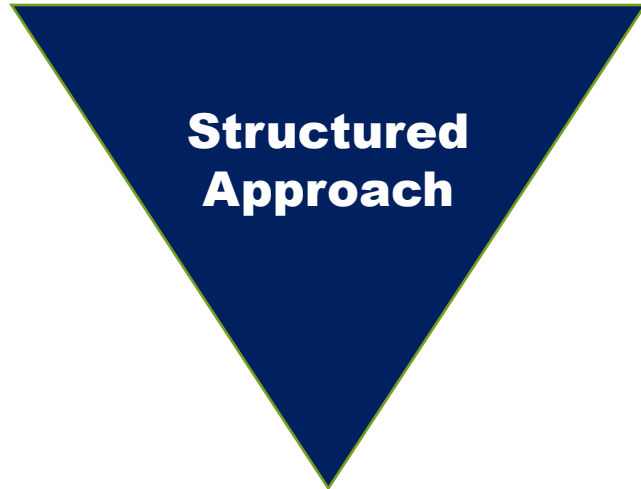
Technology

Understand

Cybersecurity Risk

Manage

Reduce

Approaches to Security

/// **Security Is a Journey**
Not a Destination

The only constant when it comes to technology is change. Change is inevitable, and as technology evolves, we must recognize that the goal of securing our environments is an unending process of learning and enhancement. Therefore, is it essential to implement security programs that can adapt and grow with your environment.

Preparing for the Journey

Dedication Over Time Is Key

The Journey Itself Brings Wisdom and Knowledge

BCNET
CONNECT

COMPUGEN
Dream. Design. Deliver.

Approaches to Security

What's next for CISOs? Staying ahead of the curve.

- Identify gaps in traits, behaviors and soft skills that will enable you to be more effective in your role.

- Focus on the future of your role by balancing your need to fight immediate fires vs. proactive risk decisions.

- Establish more-regular relationships with stakeholders that will influence your ability to become a trusted partner.

- Balance and reallocate your time toward activities that encourage business participation and decision making.

- Keep benchmarks as useful data points, but make sure your risk appetite, value management and cost optimization initiatives are what drive your decision-making process.

The Evolution of the CISO Role

Controls manager	+	Risk decision owner	+	Trusted facilitator	+	Value creator
Manage SecOps		Build IT relationships		Provide assurance		Enable business decisions (e.g., M&A)
Secure the perimeter		Assess "information" risk		Facilitate risk decisions with business owners		Manage value generation activities
Manage firewalls		Presumed owner of risks		Manage business stakeholder relationships		Executive leader

n = 129 CISOs
Source: Gartner

Gartner for IT Leaders   Follow Us on LinkedIn   Become a Client   10
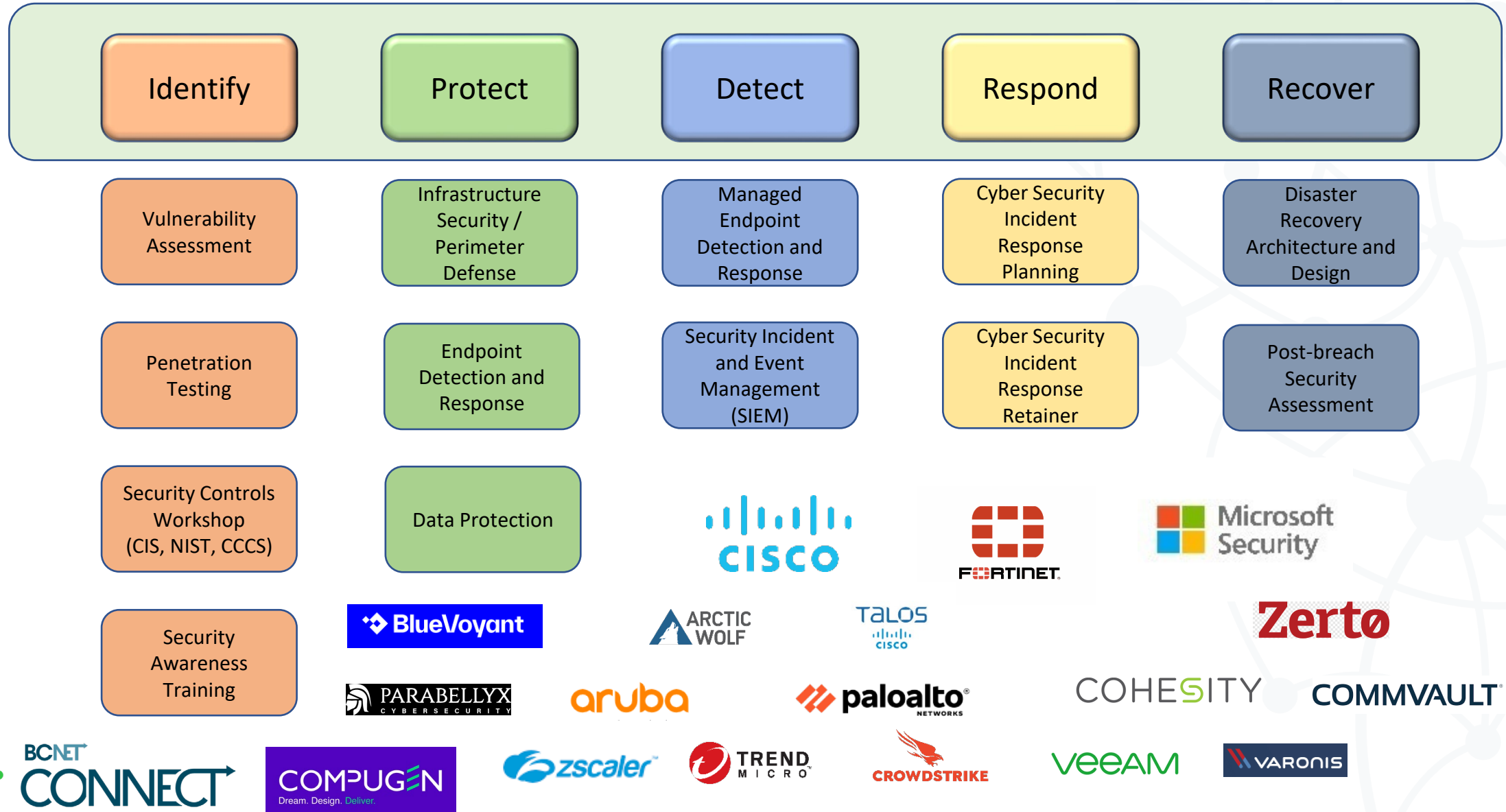
BCNET CONNECT

COMPUGEN Dream. Design. Deliver.

four-facets-of-effective-ciso-leadership.pdf (gcom.cloud)

Approaches to Security

Change is the only constant – Embrace it!

Be Creative

Partnerships are Vital

Security Solutions and Services

Identify	Protect	Detect	Respond	Recover
Vulnerability Assessment	Infrastructure Security / Perimeter Defense	Managed Endpoint Detection and Response	Cyber Security Incident Response Planning	Disaster Recovery Architecture and Design
Penetration Testing	Endpoint Detection and Response	Security Incident and Event Management (SIEM)	Cyber Security Incident Response Retainer	Post-breach Security Assessment
Security Controls Workshop (CIS, NIST, CCCS)	Data Protection			
Security Awareness Training				

- Transition to SASE
- Identity and Authentication
- Reduce Attack Surface

- Security Road Mapping
- Security Governance
- Security Assessment Services

"The important thing is that we stick together!"

Buzz Lightyear

IoT in Education

What is IoT?

- IoT are literally billions of, historically unintelligent physical devices, that are now being connected to data networks via the Internet.

- These devices are made intelligent by embedding sensors and compute that communicate real-time data without human intervention.

- They communicate with themselves, IoT applications, and platforms – and enable business outcomes via the intelligence generated through data analytics.
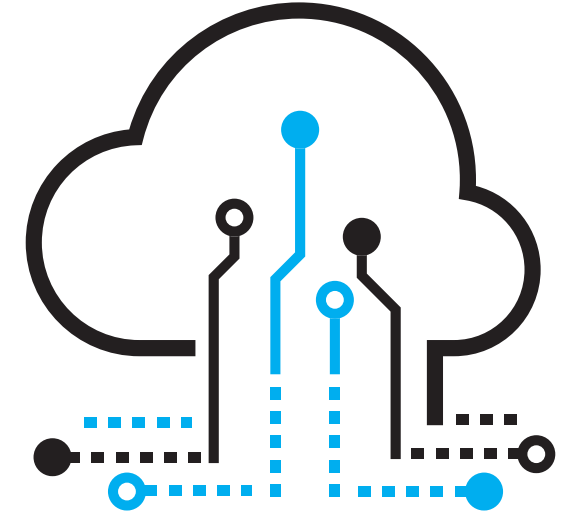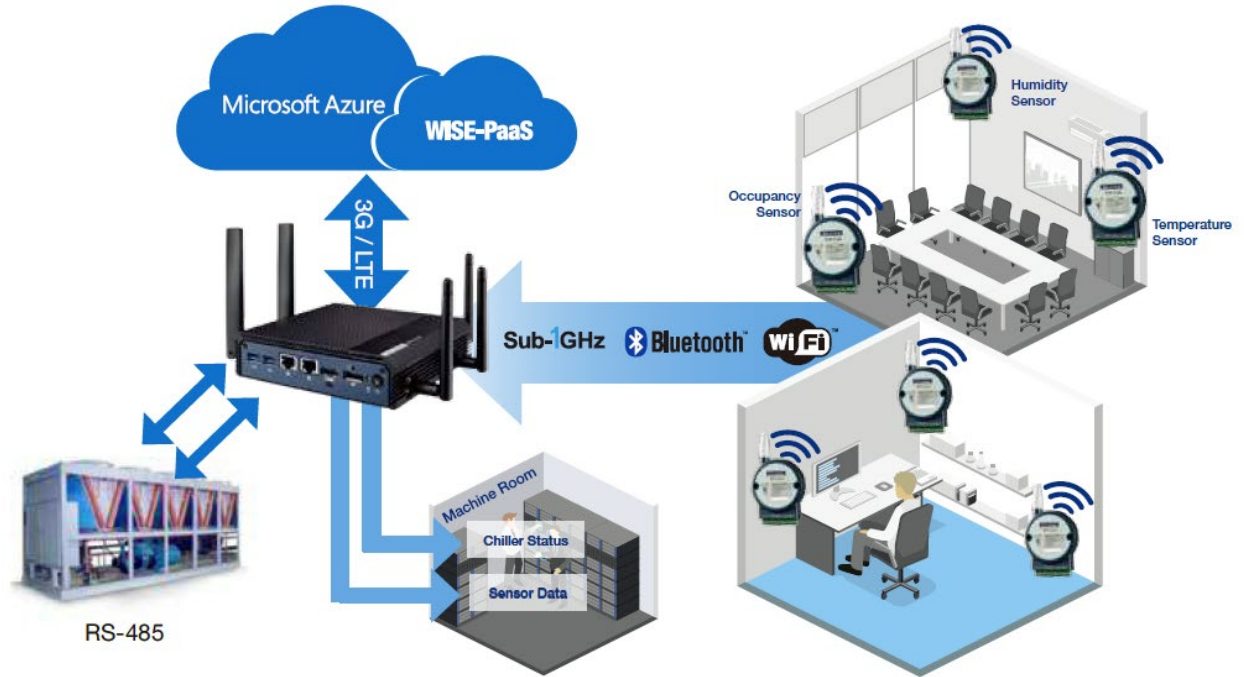
IoT

IoT Examples

Enterprise equipment used to control facility systems

- Connected HVAC
- Smart Lighting
- Video Cameras
- Door Sensors
- Alarms
- Badge Readers

IoT Examples

Learning tools
- Enabling devices, used by students with special needs
- Laboratory equipment
- Projectors
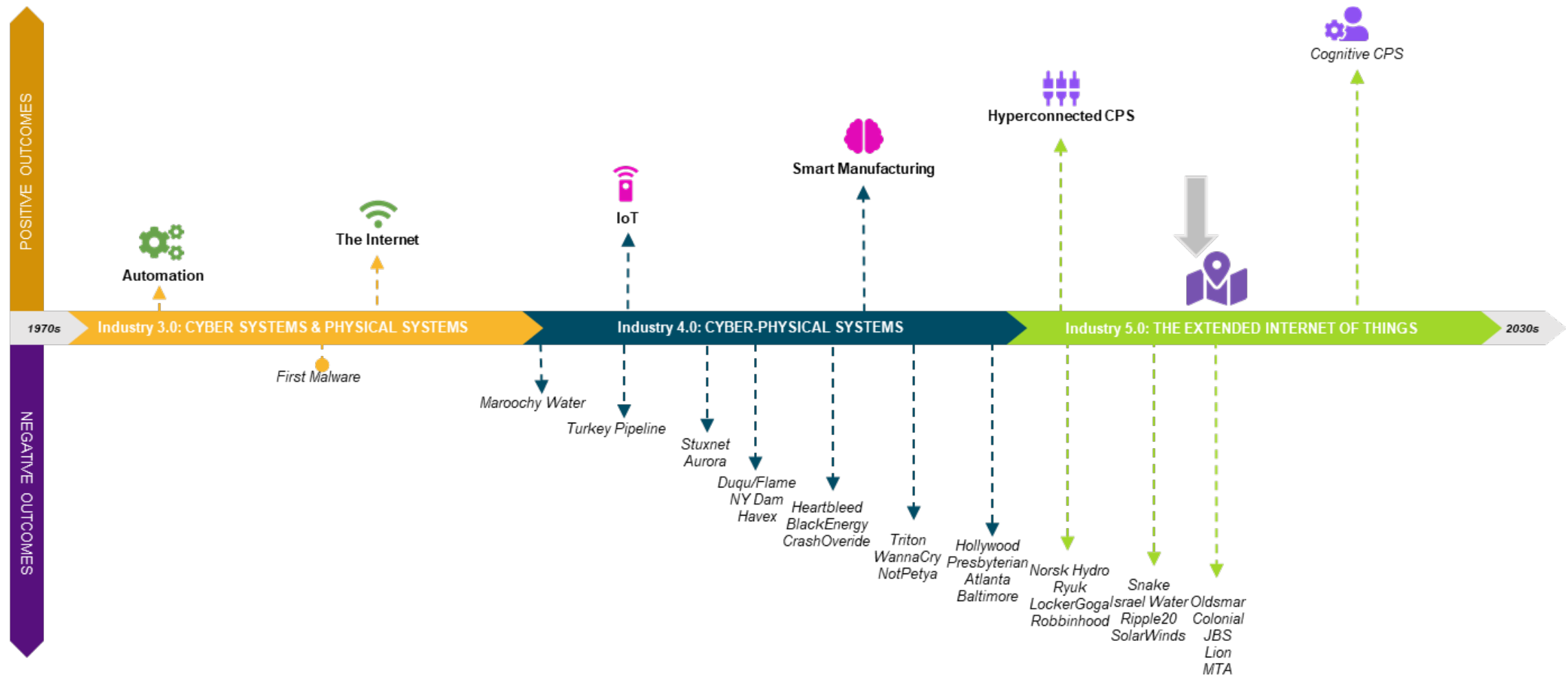- Interactive whiteboards
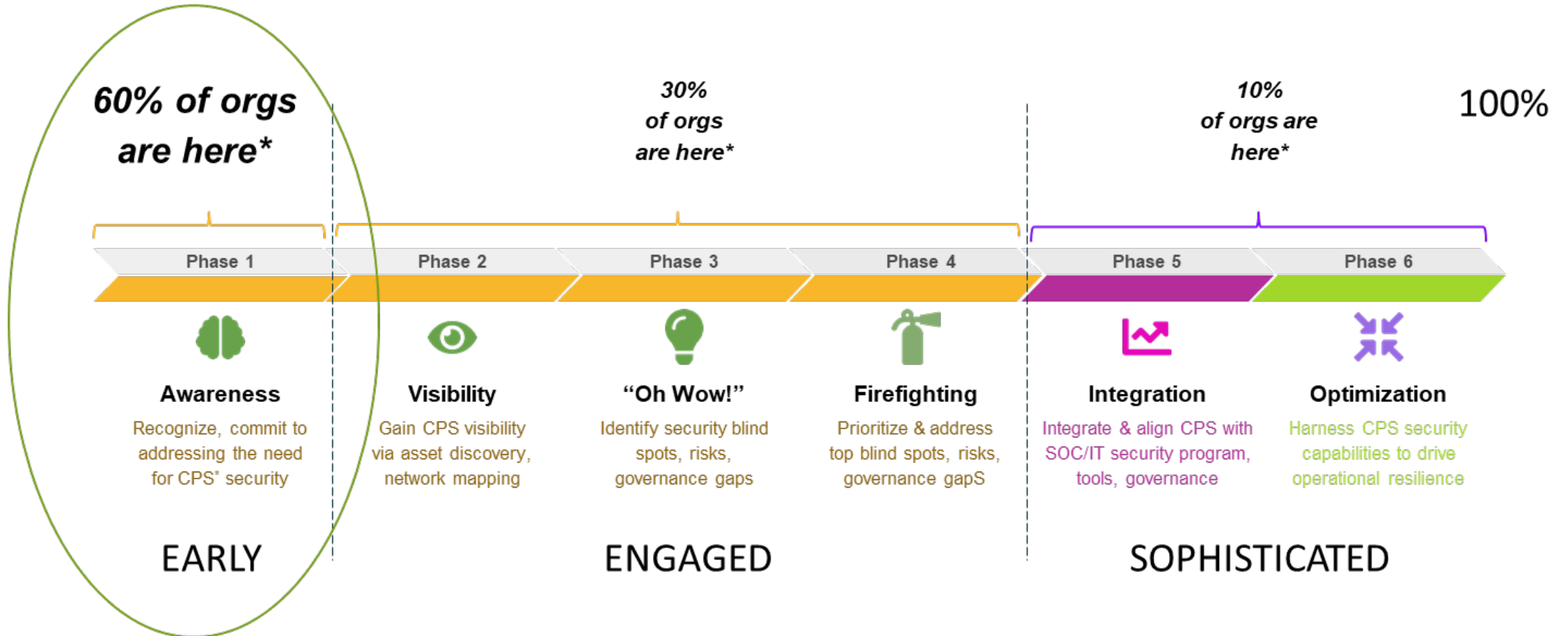- Document cameras

IoT Examples

Consumer technologies
- Connected vending machines
- Connected refrigerators
- Fitness/smartwatches
- Cloud-based assistants
  - Alexa
  - Google home
- Medical devices
  - Glucose level monitors

IoT threats are increasing in scale and velocity

The Journey – Where is your xIOT Security Program?

60% of orgs are here*

30% of orgs are here*

10% of orgs are here*

100%

| Phase 1 | Phase 2 | Phase 3 | Phase 4 | Phase 5 | Phase 6 |

Awareness
Recognize, commit to addressing the need for CPS* security

Visibility
Gain CPS visibility via asset discovery, network mapping

"Oh Wow!"
Identify security blind spots, risks, governance gaps

Firefighting
Prioritize & address top blind spots, risks, governance gapS

Integration
Integrate & align CPS with SOC/IT security program, tools, governance

Optimization
Harness CPS security capabilities to drive operational resilience

EARLY

ENGAGED

SOPHISTICATED

* CPS = Cyber Physical Systems
[1]Source: Market Guide for Operational Technology Security, Gartner, 2021

BCNET CONNECT

COMPUGEN
Dream. Design. Deliver.

Steps to Mitigate Security Threats

Asset discovery

Identify all your IoT assets to build the right security strategy

Network segmentation

Integrate existing security tools such as Network Access Control and Endpoint Detection and Response to Isolate networks and build secure zones to avoid attacks to spread

Live threat detection

Detect IT intrusions and abnormal IoT behaviors to maintain process integrity

Integrate SOC

Gain a holistic view on security events to ease investigation & remediation

We are here to help.

Salman Alibhai
Solution Specialist
salibai@compugen.com

Inder Singh
Advanced Solutions Digital Architect
isingh@compugen.com