Canadian Nuclear Laboratories | Laboratoires Nucléaires Canadiens

Managing Cyber Insider Threat at CNL

Yanick Dube, Nuclear Cyber Security

- September 2024

Profile

Canadian Nuclear Laboratories (CNL)

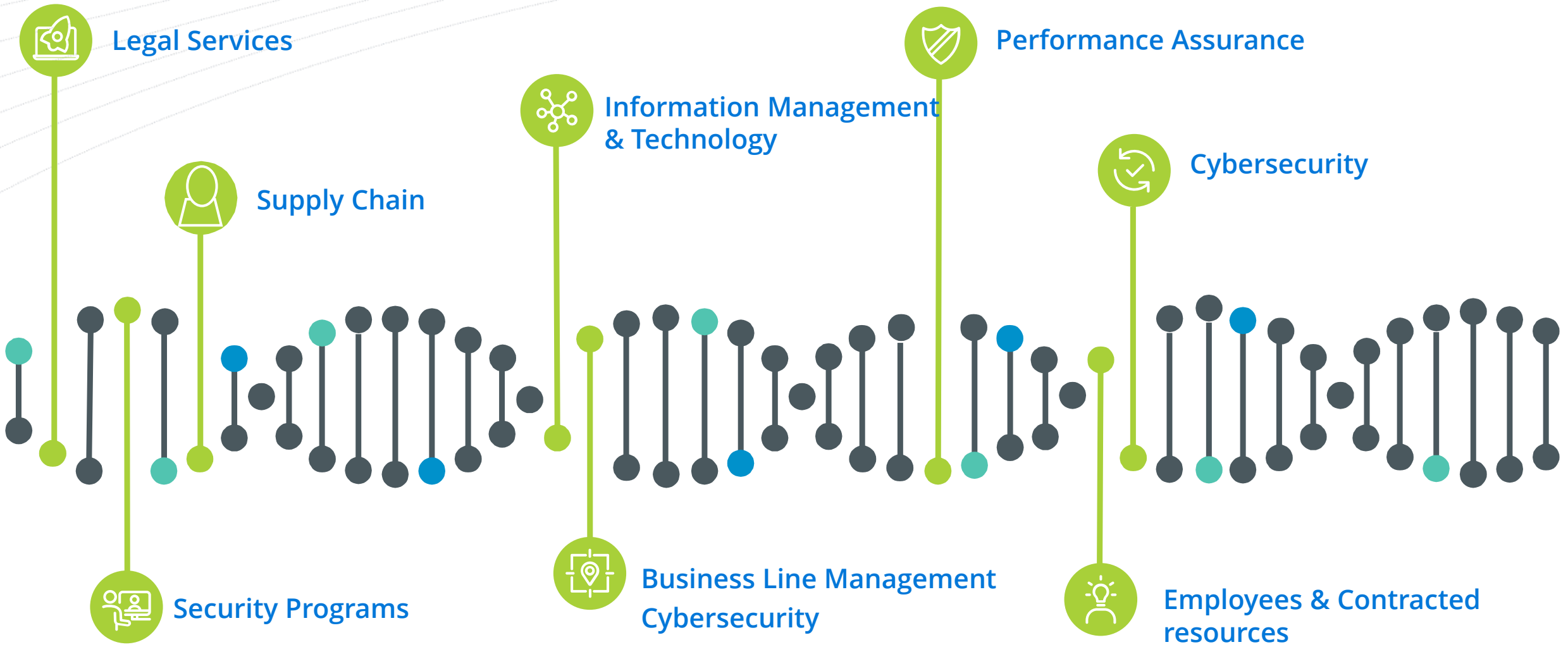
- GoCo Operator for AECL
- Science & Technology
- Environmental Remediation
- Campuses in 3 provinces
- Operations across all Canada
- 4,500 employees & contingent workers
- ~20% workforce working remotely

“Everyone has a share”

Milo Minderbinder

(…definitely not talking about insider risk…)

Managing Cyber Insider Risk

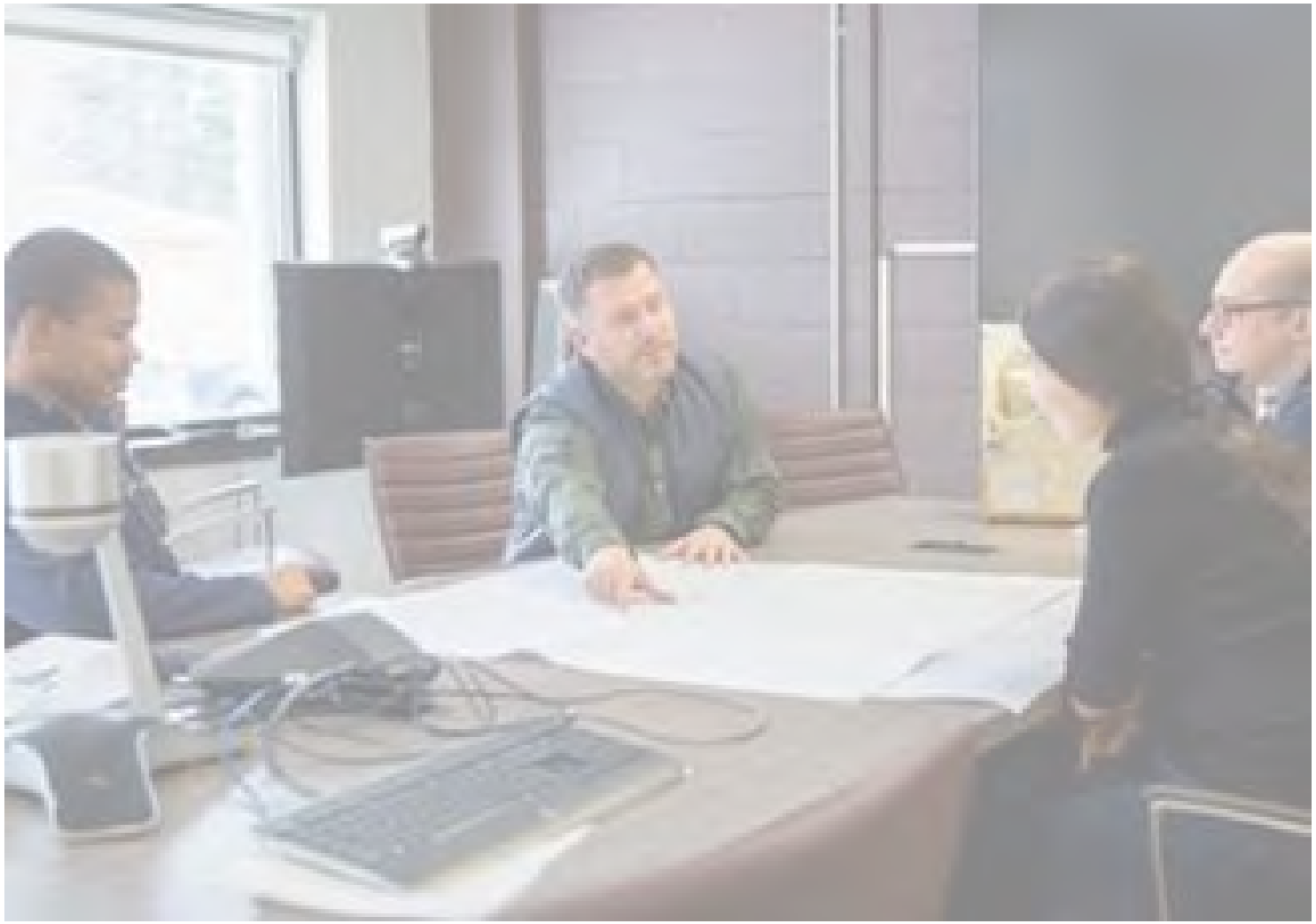


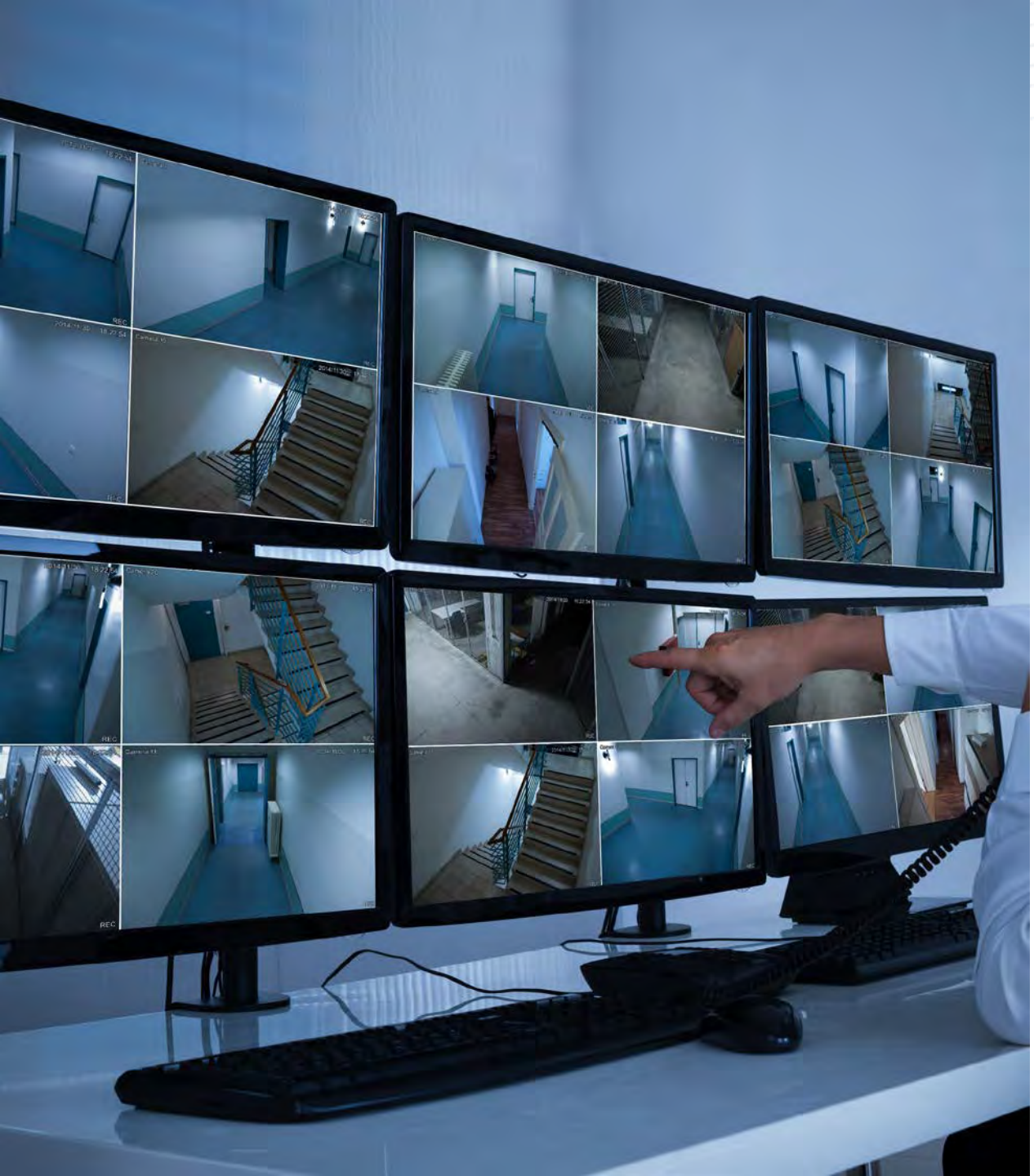
Legal Services

- Employee Code of Conduct
- Supplier Code of Conduct
- Third Party Due Diligence

Emphasis placed on **screening** organizations & resources who will have CNL **network and/ or access to a site**.

Screening can result in
- Do not hire/ contract
- Hire/ contract with mitigating measures
- Hire/ contract

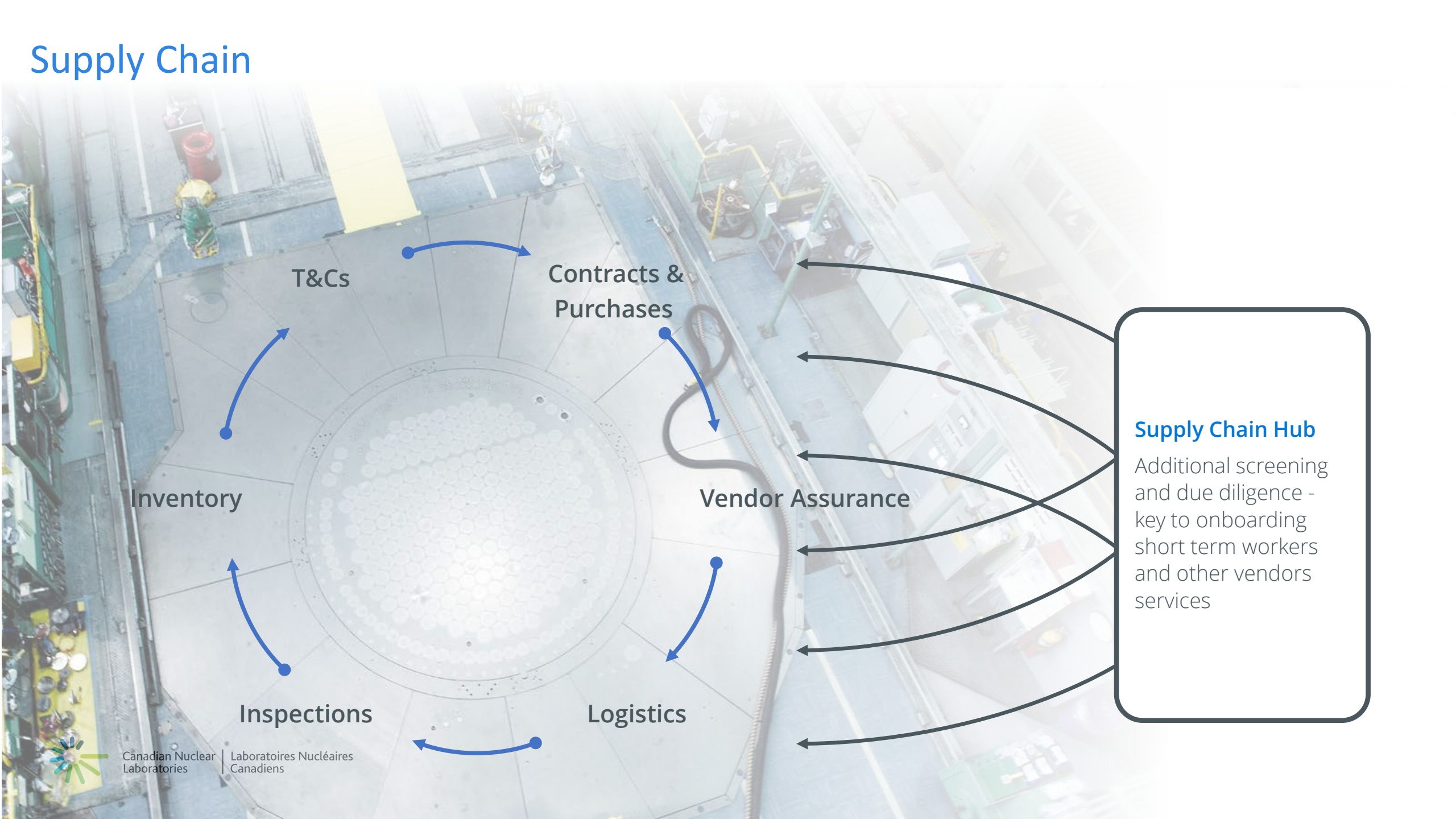




Security Program & Performance Assurance

- Security Clearance Screening
- Security Culture
- Monitoring & Response
- Human Performance

Supply Chain

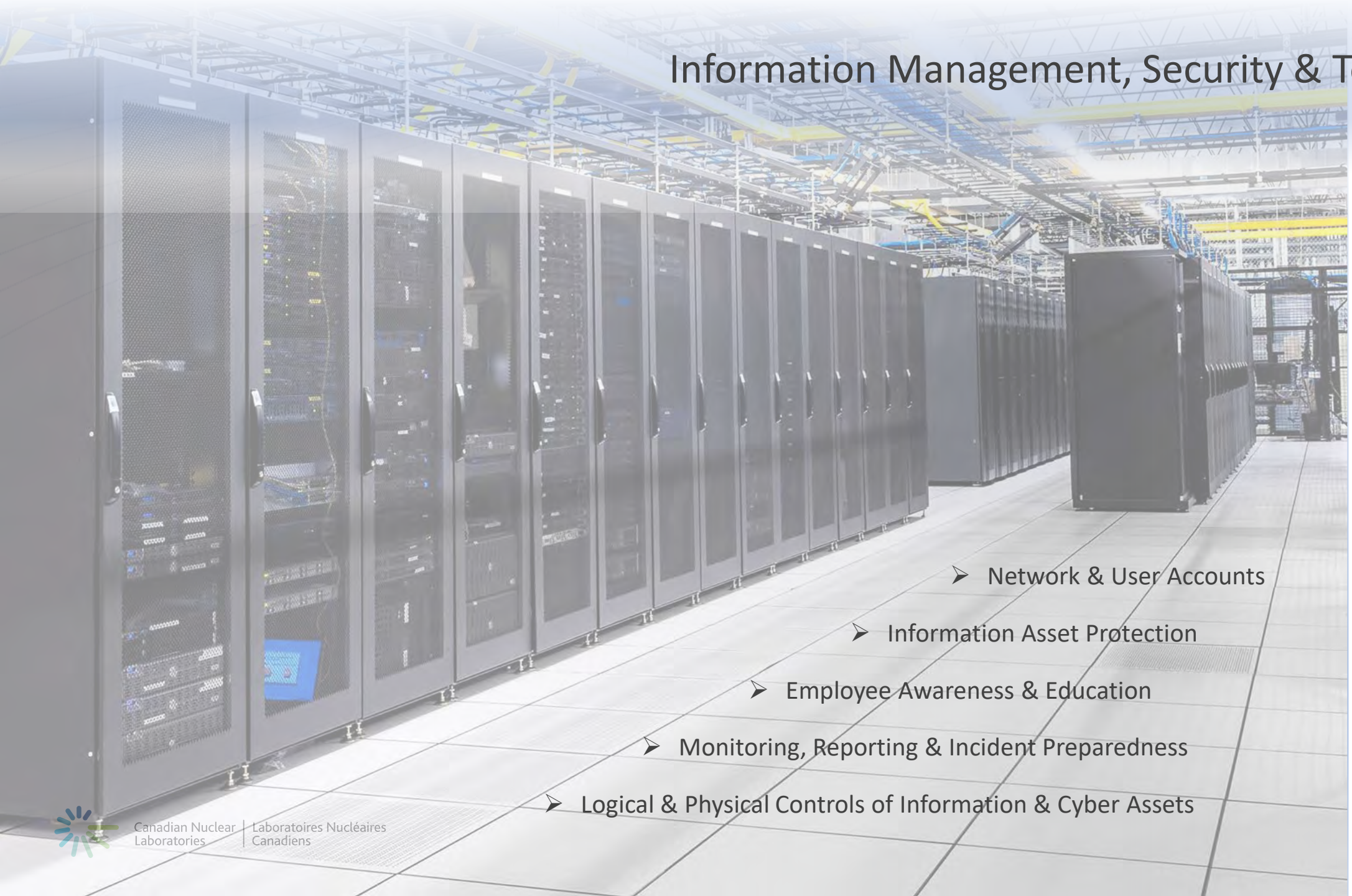


Supply Chain Hub

Additional screening and due diligence - key to onboarding short term workers and other vendors services

Canadian Nuclear Laboratories | Laboratoires Nucléaires Canadiens

Information Management, Security & Technology



- Network & User Accounts
- Information Asset Protection
- Employee Awareness & Education
- Monitoring, Reporting & Incident Preparedness
- Logical & Physical Controls of Information & Cyber Assets

Line Management & Employees

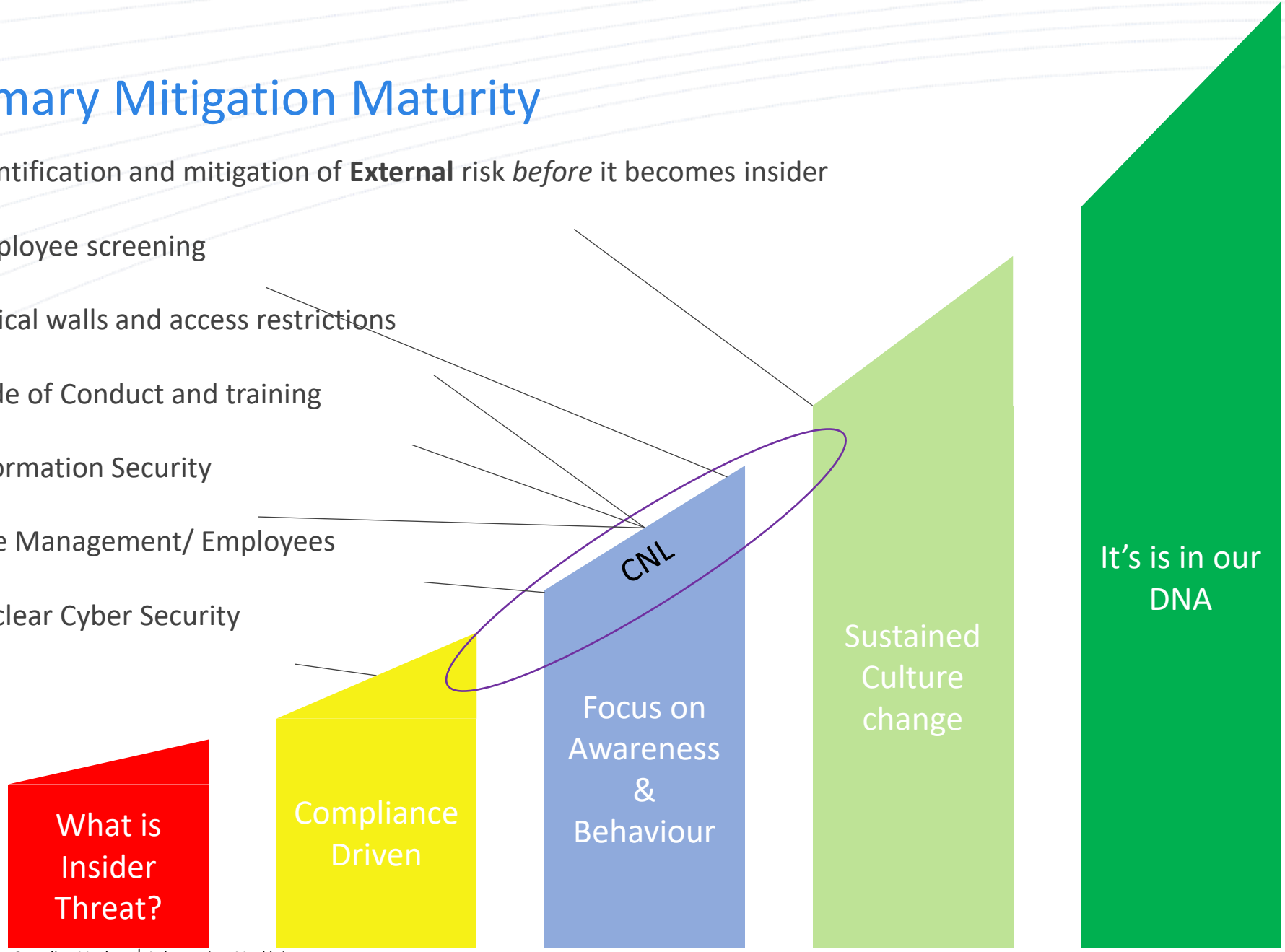
- Define Business Objectives
- Engaged in risk screening activities
- Identify Need to Know
- Responsible for access & distribution of information
- Observation and Coaching
- Day-to-Day interface with “outside world”

About Cyber Insider Risk

Making Sense of the Puzzle Pieces

Primary Mitigation Maturity

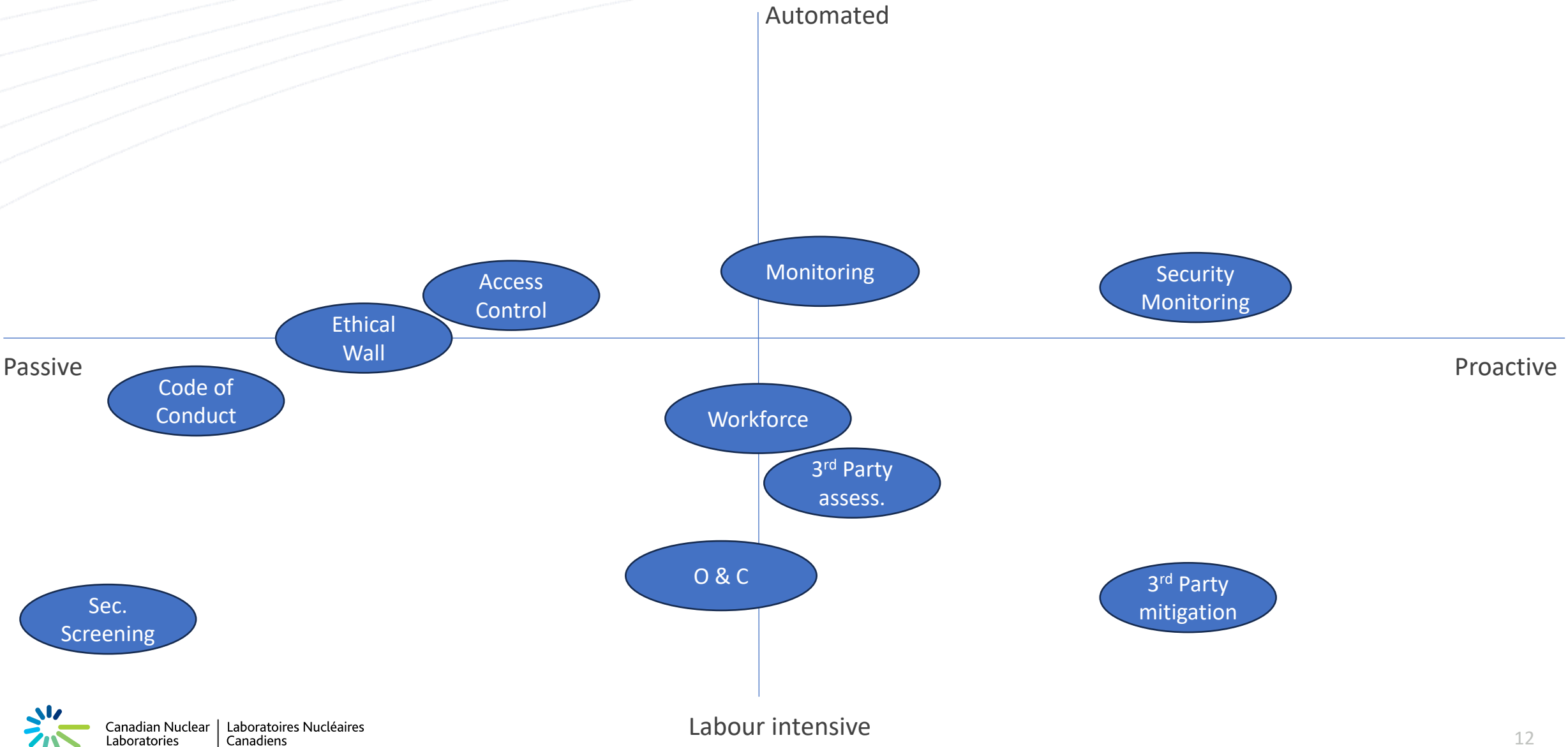
- Identification and mitigation of **External** risk *before* it becomes insider
- Employee screening
- Ethical walls and access restrictions
- Code of Conduct and training
- Information Security
- Line Management/ Employees
- Nuclear Cyber Security



Secondary Mitigating Elements

- Network Account Mgmt
- Guards and security monitoring
- Observation & Coaching (O&C)

Opportunity Map



In Summary & Next Steps for CNL

1) Formalize Insider Cyber Threat Program elements

2) Embed Cyber elements in existing processes

3) Improve employee awareness and toolkit

4) Increase leverage of existing, and adopt new tools

Q & A