Cybersecurity for DS: How *NOT* to get *HACKED!*

Cybersecurity Foundations for Developmental Services Organizations

Asurtec

June 11th, 2026

Today's Speaker

Scott Trevithick

Chief Executive Officer

Asurtec

Scott is the CEO of Asurtec, a digital empowerment partner for not-for-profit community organizations. He has worked as a technology advisor and implementer for community organizations for over two decades.

Today's Objectives

1. Introduce CyberSecure Canada's Baseline Controls and certification program
2. Help leaders understand how this can benefit them and why it's important
3. Know what the Baseline Controls have to offer leaders in various roles (EDs, Finance Directors, Privacy Officers, IT leads)
4. Understand where the CyberSecure Canada Baseline Controls fit in relative to enterprise frameworks
5. Know how to get started, what questions to ask and what steps to take
6. Understand the overall 4-step process from gap analysis to optional Cybersecure Canada certification

Introduction to Cybersecurity & CyberSecure Canada

Cybersecurity: A Herculean Challenge

Community Livings face a nearly impossible challenge: they face the same increasingly dangerous cybersecurity threats as hospitals and larger for-profit firms, but they have a fraction of the resources of these organizations.

Community Livings need an approach to cybersecurity that is straightforward, practical, and low-cost, with a high return on investment

What is CyberSecure Canada

CyberSecure Canada is a federal certification program for small to medium sized organizations built on the Canadian government's baseline cybersecurity controls.

It is perfectly suited to organizations with < 500 employees seeking to protect themselves against cyber threats.

What the Controls Cover

Organizational and Technical Controls

Baseline covers both organizational and technical controls forming a complete cyber resilience model.

Examples of Controls

Baseline controls include key areas like an incident response plan, automated patching, multi-factor authentication, policies, back-up and encryption for security.

Multiple Leadership Audiences

Controls speak to Executive Directors and CEOs, Finance Directors, Privacy and Security Officers and IT pros.

Broad Scope

Baseline spans IT Infrastructure, mobile, cloud, vendor risks, emphasizing governance, behavior, prevention and incident handling.

The CyberSecure Canada Baseline Controls

Provide a Broad, Balanced Framework

The Baseline Control areas create a balanced framework spanning **people**, **process**, **governance**, and **technology**.

Promote a Mature Response to Risk

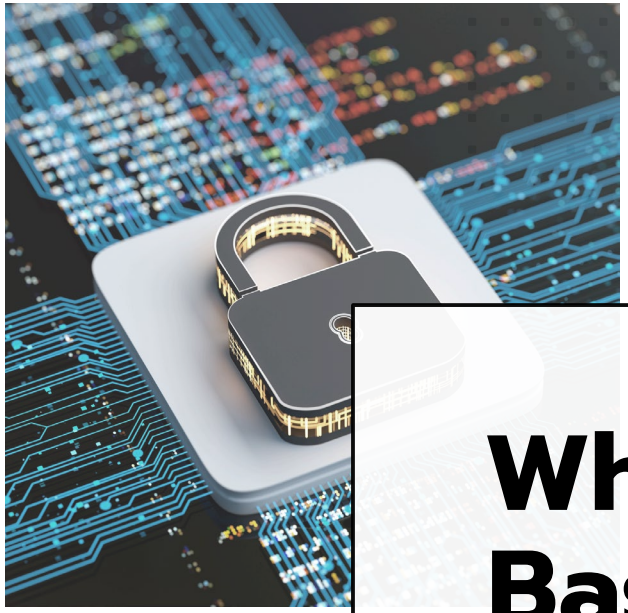
Controls support **prevention**, **detection**, **response**, and **recovery** in an integrated cybersecurity approach. Preparedness for incidents that are expected to happen.

Support a Framework for Readiness Planning

Framework supports prioritization, and **phased implementation** for organizational cyber readiness. It can be partially implemented using internal resources and fully with a qualified partner.

Why This Is Important For You & Your Organization

Asurtec



Why the Baseline Controls Matter

Tailored for Small and Medium Organizations

The baseline controls are designed specifically for Canadian organizations with fewer than 500 employees.

Efficient Cybersecurity Effort

Applying the 80/20 (vital few) rule allows organizations to gain 80% of the benefits from 20% of the cybersecurity effort, easing resource burdens.

Addresses Real Risks

Cybercrime poses significant risks: financial loss, reputational damage, and disruptions to client services.

Cybersecurity can Threaten the Entire Organization

Cybersecurity impacts service delivery, confidentiality and privacy, and stakeholder confidence – some cyber incidents have been fatal for for-profit companies.

Be Proactive, not Reactive

Many organizations wrongly assume that they are not a target as they are a not-for-profit, not a bank or hospital. The get serious about cybersecurity only *after* a serious incident.

Why Cyber Security Matters

For Executive Directors and CEOs

Leadership Accountability

Baseline Controls place cybersecurity accountability at the senior leadership level, emphasizing management responsibility.

Risk and Governance Focus

The framework begins with governance and risk-scoping. Organizations identify their size, IT and cybersecurity spending and primary cyber threat (likely, crime).

Cyber Incident Preparedness

Leaders must ensure plans for responding to and recovering from cyber incidents are in place with clear roles and escalation protocols.

Strategic Organizational Resilience

Cybersecurity is framed as a strategic risk area critical for service continuity, stakeholder trust, and operational resilience.

For Finance Directors, Privacy Officers and IT Teams

Financial Implications

Cyber threats often target financial functions, have immediate financial impacts, and preparedness requires budgeting for IT security expenditures.

Privacy Harm & Incident Response

Privacy roles focus on assessing confidentiality, integrity, and availability (CIA) of data and managing communication breaches effectively.

IT Team Guidance

The Baseline controls provide numerous recommendations aligned to best practices for managing IT infrastructure, devices and user accounts.

The Baseline Controls are a "Goldilocks" Starting Point

"Just right"

The Canadian baseline controls offer a structured yet manageable approach ideal for small- to medium-sized organizations with up to 499 employees and average cybersecurity risk.

SMB Appropriate Framework

Baseline controls provide essential security guidance without the high costs of larger frameworks.

Why Not Enterprise Cybersecurity Frameworks?

NIST, CIS, ISO/IED 27001 and Centre for Internet Security (CIS) frameworks are designed for complex, high risk environments and enterprises. They require professional third-party support. They are costly and complex to implement and therefore impractical for most DS sector organizations.

CyberSecure Canada Baseline Controls

Getting Started...

Asurtec

First Steps

1

Framework Fit Assessment
Are we the right fit? Are we under 500 employees, do not process high volume financial transactions, hold high value data or have unusually complex security needs?

2

Identify Everything you need/want to Protect
Inventory all in-scope assets including computers, servers, network devices, desktop, server and cloud applications, and confidential information to understand risk exposure.

3

Assess Potential Harm and Injury
Evaluate harm to confidentiality, integrity, and availability using a scale of very low to high impact. *If x were compromised, what would the consequences be?*

4

Identify Primary Threats and Assign Ownership
Assess spending on IT and cybersecurity as % of budget. Recognize primary cyber threats and assign leadership for cyber security within the organization.

Note: **For items where the potential harm or injury from a compromise would be *high*, measures *in excess of* the baseline controls are recommended.**

Prioritize Foundational Controls

Review essential controls like incident response planning, multi-factor authentication, backups, password policies, and automatic patching and target these early on.

Document Decisions and Plan

Record business rationales for controls not fully implemented to support staged, realistic improvement plans. *In the first 6 months, we'll do x, y, and z and in the second 6 months...*

Don't Attempt Everything At Once

Cybersecurity is a Journey, Not a Destination

Commit to Continuous Improvement

Organizations should plan for ongoing investment and resourcing to progressively enhance cybersecurity. Threats continuously evolve; your cybersecurity should, too.

Path to Cybersecure Canada Certification (optional)

1 **Gap Analysis**

Gap Analysis identifies security, policy, and documentation gaps comparing current state to baseline requirements.

2 **Remediation Plan**

Remediation Plan prioritizes fixes based on risk, effort, sequencing, and ownership for effective cybersecurity improvements.

3 **Remediation Implementation**

Remediation implementation implements technical changes, policy updates, training, and documentation improvements.

4 **Certification Readiness**

Certification Readiness prepares evidence, validates controls, and readies the organization for independent certification.

“You’re Richer Than You Think”

(i.e., some boxes might be checked already)

Existing Security Practices

Many organizations have partial security controls like multi-factor authentication and backup practices already in place.

Build on What You Already Have

The baseline helps organize and strengthen existing controls into a coherent and auditable cybersecurity framework.

Reduces Anxiety & Encouraging Progress

Recognizing existing strengths reduces anxiety and builds confidence and momentum. You got this!

***Note:* The Baseline Controls recommend that you purchase Cyber Insurance for incident management** (excellent advice, but be advised…)

Baseline Controls & Cyberinsurance

The CyberSecure Canada Baseline Controls offer practical, right-sized cybersecurity but insurers may ask about enterprise-level protections.

Baseline controls may not fulfill all cyber insurance questionnaire requirements, especially specific, security-focused applications.

Limitations

Insurer questions often include very specific measures, e.g., endpoint detection and response (EDR) and Data Loss Prevention (DLP), beyond the general baseline measures.

Specificity

Baseline controls are excellent but be aware that some insurers may ask about, even require, more specific, and complex cybersecurity applications.

Be prepared...

CyberSecure Canada Baseline Controls

… in summary

- The controls are an excellent, effective and practical approach to cyber security.
- Many controls can be implemented without outside expert assistance.
- An experienced implementation partner can help you implement *all* the controls
- Implementing the controls is a strong, defensible, high ROI approach to protecting your organization

Questions?

How Community Living Organizations Can Leverage Cybersecure Canada

Questions about this presentation, and how we can help you on your cybersecurity journey can be directed to:

Scott Trevithick
Chief Executive Officer
Asurtec Solutions
E: strevithick@asurtec.com
P: 289-907-0553
W: www.asurtec.com