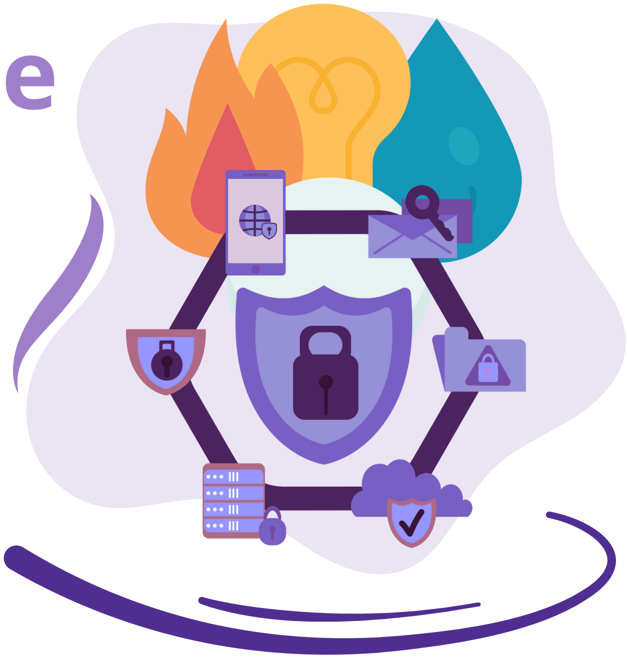
maximus Moving Canadians, Technology, and Government Forward

Is Your Infrastructure Ready for 2026 Cybersecurity Threats?



Maximus + QSI Security are moving government forward with smart solutions for the Canadian Utilities Sector

Canadian utilities are facing targeted attacks with real operational and reputational consequences. The Canadian Centre for Cyber Security warns that ransomware remains the top threat to critical infrastructure this year, with state-sponsored activity becoming more aggressive. **The impacts of these growing utility cyberattacks are threefold:**

1 Public trust

Utilities carry a duty to protect essential community services. Vulnerabilities and attacks erode community confidence and the trust placed in public institutions.

2 Service delivery

Attackers can shut down or manipulate water, energy, and critical infrastructure, affecting entire communities and cascading across borders.

3 Compliance penalties

Regulatory bodies (such as provincial energy boards) have the authority to hold accountable the individuals or entities that breach their statutory duties.

Recent Canadian incidents show the scale of the threat:

- In 2025, a provincial power utility experienced a ransomware attack that disrupted smartmeter communications for roughly 280,000 customers.
- Elsewhere, hacktivists manipulated water pressure, altered an oil & gas tank gauge, and interfered with grain drying controls.

Let's connect:
maximuscanada.ca

Maximus has partnered with QSI Security to offer comprehensive cybersecurity capabilities for Canadian utilities.

maximus Moving Canadians, Technology, and Government Forward

How Maximus + QSI strengthen & protect Canadian utilities

Maximus + QSI protect utilities working in petroleum, water, power, hydroelectric, sewer, electricity, natural gas with cybersecurity experience spanning major Canadian Mining Operations to global Industrial Manufacturing.

Real World Application | Real Results

WHAT | Continuous protection

A comprehensive Security Operations Centre monitors your environment 24/7/365, aligned with industry controls, including incident triage, threat hunting, and automated response capabilities.

HOW | Clear understanding of your risks

Advanced surveillance tools, behaviour analytics, and dark web monitoring to detect and correlate malicious activity. Detailed assessments of vulnerabilities empower organizations to close the gap and fulfil audit requirements.

NOW | Coordinated incident response

Rapid containment and support to minimize downtime and operational disruption. Real-time and automated threat containment, incident response playbooks, and remediation support, ensuring operational readiness and continuous protection.

WOW | Expert Profiles

Maximus + QSI brings deep, niche expertise that generalist IT firms lack. Our roster of cybersecurity professionals includes:

- **Industrial Control Systems (ICS) and Operational Technology (OT) Security Architects:** Specialists in utility/industrial hardware
- **Senior Threat Hunters:** Providing 24/7 Security Operations Monitoring
- **Incident Response Leads:** Active response team in case of incidents.
- **Governance, Risk, and Compliance Specialists:** Ensuring utilities are audit-ready and prepared to confidently meet their compliance needs.

Maximus understands public-sector operations, at the municipal, provincial and federal level with over 20 years of supporting utilities and energy sector organizations.

QSI brings specialized IT | OT security expertise. The exclusively-Canadian team provides continuous monitoring and incident response for critical systems.

> “When Canada invests in strong safeguards, we prevent against costly disruptions, strengthen service continuity, and uphold the responsibility that public sector organizations have to the people they serve.”
>
> Veronica Mustoe
> Vice President, Privacy & Security, Maximus

Let’s connect:
maximuscanada.ca