Electricity Canada | Électricité Canada

Technology Trends 2026

Contents

About Electricity Canada

Founded in 1891, Electricity Canada is the national forum and voice of Canada's evolving and innovative electricity business. Through its advocacy efforts, the association supports the regional, national, and international success of its members.

Electricity Canada members generate, transmit, and distribute electrical energy to industrial, commercial, residential, and institutional customers across Canada. Members include integrated electric utilities, independent power producers, transmission and distribution companies, power marketers, manufacturers, and suppliers of materials, technology, and services.

Acknowledgments

Electricity Canada recognizes the significant contributions of others in the preparation of the second annual Technology Trends report.

A special thanks to all contributing authors and committee leaders: Ian Fish, Vice President of Digital Technology of Manitoba Hydro; Humie Woo, Vice President of Information Technology of Toronto Hydro; Jennifer Pederson, Director of Business Solutions of SaskPower, and the Electricity Canada Technology Committee members, for their efforts in developing this report.

Preface: Letter from the Chair

The Canadian electricity sector stands at a pivotal moment. The technologies reshaping our industry are evolving faster than ever, driven by the convergence of artificial intelligence, data analytics, automation, and digital collaboration. These innovations are redefining how we operate, how we serve our customers, and how we safeguard the reliability and security of the grid that underpins Canada's economy and quality of life.

Senior technology staff in the industry see firsthand how technology has become central to achieving organizational excellence and resilience. The themes explored in this year's *Technology Trends 2026* report look forward to growing opportunities, but also those risks closely associated with them. They are citizen development, artificial intelligence (AI), robotics and drones, major systems migrations, and cybersecurity. These focal areas reflect the reality that transformation is no longer optional; it is strategic. Each of these trends represents a cornerstone of the digital utility future. Together, they illustrate how our sector is responding with agility, foresight, and collaboration.

Across Canada, utilities are empowering employees to innovate through citizen development, adopting low-code and no-code tools that accelerate problem-solving and strengthen partnerships between IT and business. Artificial intelligence, robotics, and drone technologies are improving grid reliability, supporting workforce safety, and enabling real-time insight and automation. At the same time, utilities are undertaking major systems migrations (modernizing foundational platforms and embracing cloud technologies) to position their organizations for a more connected and data-driven future. Cybersecurity remains a constant and critical priority, as utilities work collectively to protect the integrity of Canada's energy systems against increasingly sophisticated threats.

While the pace of change can be daunting, it also brings opportunity. The collaborative work of Electricity Canada's Technology Committee demonstrates that our sector's strength lies in shared learning and a unified commitment to innovation. Through open dialogue, collective problem-solving, and industry alignment, we are ensuring that utilities across the country have the tools, governance, and digital strategies to lead confidently into the next decade.

On behalf of the Technology Committee, I would like to thank all contributing authors, committee members, and Electricity Canada for their leadership in producing this report. Your efforts not only showcase the breadth of innovation across our industry but also provide valuable insights to guide executive decision-making in a time of rapid technological and operational change. The Committee would especially like to thank Ian Fish, for his service to the industry and contributions over the years.

As leaders, we have a shared responsibility to harness technology responsibly, invest in our people, and build an electricity system that is more sustainable, secure, and resilient. Together, we are shaping a digital foundation that will empower Canada's energy future for generations to come.

Jennifer Pederson
Chair Technology Committee
Director of Business Solutions,
SaskPower

Humie Woo
Vice-Chair Technology Committee
Vice-President Information Technology,
Toronto Hydro

Introduction

The Canadian electricity sector is navigating a period of rapid change as utilities adapt to evolving operational, technological, and regulatory demands. Organizations are exploring new ways to empower their workforce, improve operational efficiency, and enhance grid resilience.

This report explores four major technological trends that will impact electric utilities over the coming years, all of which highlight common themes of innovation, agility, and data-driven decision-making. Across citizen development, AI, robotics, and drone deployment, major systems migrations, and advanced cybersecurity, utilities are fostering collaboration, enhancing operational efficiency, and building resilience to navigate a rapidly evolving energy landscape.

Citizen development is enabling employees outside of IT to create reports and applications, fostering innovation and reducing reliance on centralized IT teams. At the same time, artificial intelligence, robotics, and drones are being deployed to optimize grid operations, improve safety, and enhance climate resilience. Utilities are also undertaking major systems migrations, modernizing enterprise platforms and cloud-based solutions to unlock new capabilities, improve data quality, and support long-term operational agility. Across all these efforts, cybersecurity remains a critical focus, with advanced frameworks and AI-enhanced monitoring helping to protect the grid from increasingly sophisticated threats. Together, these approaches position organizations to operate more efficiently, respond to customer and regulatory expectations, and build a foundation for continued modernization and resilience.

Citizen development: Empowering business innovation

Citizen development: Empowering business innovation

Contributing authors:

- **Rob Anderson**, Manager, Innovative Solutions, SaskPower
- **Jennifer Pederson**, Director, Business Solutions, SaskPower

In the rapidly evolving technology landscape, organizations are continuously seeking innovative ways to address the growing demand for time saving and cost-effective solutions. One of the emerging strategies to meet this demand is to encourage and facilitate employee led development. Using citizen development to enable self-service will foster a culture of innovation and agility within your organization.

What is citizen development?

A citizen developer is an employee who builds reports or applications for their own use or for others within the organization. Citizen developers use low-code and no-code technologies and platforms which do not require deep programming knowledge. Citizen development is intended for employees who work in business units outside of IT, regardless of their prior technology or programming experience. The goal is to enable more self-service tools and technologies for people of all backgrounds.

Opportunities

Self-service outside of IT happens at companies of all sizes with or without the knowledge or permission of an IT department. IT should take the opportunity to guide employees towards secure, approved technologies for self-service. Citizen development offers numerous benefits for businesses to innovate and respond to growing demands:

- Educate employees on how to self-serve while following IT best practices and industry standards.
- Accelerate digital transformation with robotic process automation.
- Reduce burden on IT departments while fostering a culture of innovation and agility.
- Troubleshoot issues and receive guidance with low-code and no-code tools using generative AI tools like ChatGPT or Microsoft Copilot.
- Build a bridge between IT and the business to increase visibility and gain a mutual understanding of common issues and challenges.
- Replace expensive large scale enterprise systems with fit for purpose minimum viable products.
- Mitigate the risk of the business using insecure and unapproved technologies.

Challenges and risks

While citizen development offers great potential, it's also essential to be aware of the challenges and risks to ensure its successful implementation:

Shadow IT: The business can be hesitant to involve IT due to perceptions of long wait times, strict rules or conflict over requirements. The shift of the relationship between IT and the business to one with openness and transparency can take time. IT needs to lead and set standards while growing into a trusted partner.

Data drives results: Consider low-code/no-code platforms that can connect and integrate with your existing data platforms. For example, Power Platform is likely a good fit if your company is a user of Microsoft products. When choosing a platform, always consider the needs of your data roadmap.

Security and privacy breaches: Implement proper governance and guardrails like data loss prevention before rolling out your program. This will decrease the risk of security vulnerabilities, data privacy and data loss issues.

Build toolkits: Guide users towards simple, effective methods to accomplish their goals. Citizen developers should aim to avoid overly complex solutions. Citizen development meetings should provide demonstrations and real-world examples for members to follow.

Supporting solutions: Set clear expectations over how self-serve solutions will be supported and what IT's involvement will be. Provide scheduled availability for subject matter experts to meet with the community and answer any questions they might have. Leverage generative AI tools to help members troubleshoot.

Training and enablement: There is a need for continuous training and support to ensure that citizen developers are adequately prepared. On-demand training via platforms like LinkedIn Learning and Udemy will allow you to scale knowledge quickly without the need for in person teaching. The IT department should audit courses and provide an easy way to view the suggested training catalogue.

Continuous improvement: IT should investigate opportunities for new low-code and no-code technologies as they emerge. New functionality and its potential benefit to citizen developers should be monitored. IT should build a citizen development technology roadmap and share it with the community.

Open the door to AI: As AI and no-code tools continue to advance, the potential for citizen development to drive significant innovation and engagement within businesses will only grow stronger. It will soon be common for usable applications and reports to be built using only natural language.

Provide options to customers: Citizen development offers an opportunity for self-service, but it is not a replacement for IT. A citizen developer may initiate a project but struggle to complete it. Self-service allows for the business to gain a strong understanding of requirements and potential technology challenges, which can then be communicated to IT. Requesting assistance from IT is always an available option.

Strategic recommendations

Citizen development represents a transformative opportunity for companies to innovate and engage their workforce.

Here are steps to start citizen development at your company:

Create a framework: Document the goals and guiding principles for your program. Implement a Centre of Excellence with metrics and KPIs to audit solutions and measure progress.

Enable technology: Invest in low-code and no-code tools rather than traditional pro-code solutions.

Provide on-demand training: Ensure continuous training and audit courses to keep citizen developers updated on best practices.

Implement security guardrails: Establish proper governance to mitigate security risks and protect your company's data.

Schedule meetups: Host periodic community meetings to present new technologies and data sources, demo products and walk through how they were built and provide opportunity to ask questions to subject matter experts.

Foster a collaborative mindset: Create a discussion forum where community members can share success stories and help each other work through challenges.

Evaluate ideas: Build a survey to help members determine if a project is better suited for citizen development or traditional IT support.

Subject matter experts: Train IT employees with experience in the low-code/no-code platforms and have them available to answer questions during community meetings.

Choose a model: You can choose to run a centralized model where everyone in the company is part of one community and has equal participation or a decentralized model where citizen development champions are trained to lead smaller communities for each of their respective groups.

Complete a pilot program: Conduct a pilot to understand the potential and make necessary adjustments.

Conclusion

Citizen development is a paradigm shift that allows businesses to harness the creativity and problem-solving capabilities of their workforce. By embracing low-code and no-code tools, companies can innovate rapidly, enhance security through proper governance, reduce IT backlog and foster a community of empowered citizen developers.

As AI and technology continue to evolve, the power and efficiency of no-code tools will only increase. It is important for IT and business leaders to recognize and support this movement, ensuring that the solutions developed are of high quality and aligned with best practices. By doing so, companies can increase engagement, promote innovation and ultimately achieve a more agile and responsive organization.

AI, robotics, and drones for Canadian electric utilities

AI, robotics, and drones for Canadian electric utilities

Contributing authors:

- **Clay Stooshnoff**, Senior Manager IS Applications, FortisBC
- **Gary Tong**, Director IT Modernization, Toronto Hydro
- **Etienne Avon**, Directeur architecture d'entreprise et innovation, Hydro-Québec

Overview

AI, robotics, and drone technologies are rapidly transforming the Canadian electric utility sector. These tools are being deployed to enhance grid reliability, streamline operations, improve safety, and support climate resilience. From AI-driven hazard modeling to drone-based infrastructure inspections and robotic automation in substations, utilities are embracing these innovations to modernize legacy systems and meet evolving regulatory and customer expectations.

Key drivers

Regulatory pressure: Navigating the mandate for modernization

In an increasingly regulated environment with evolving timelines, compliance, and financial requirements, utilities are leveraging AI and smart grid technologies for load forecasting, energy optimization, and emissions tracking. These tools also support the integration of renewable energy sources, helping utilities maintain operational integrity while transitioning to a more sustainable and responsive energy system.

Climate resilience: Responding to a new normal

Utilities face recurring climate threats such as wildfires, floods, heatwaves, and storms, requiring proactive, data-driven responses. They are using AI-driven predictive analytics and drone-based surveillance to anticipate equipment failures, assess damage in real time, and shift from reactive crisis management to anticipatory planning that safeguards infrastructure and communities.

Technological innovation: Unlocking new possibilities

Generative AI, edge computing, and robotics are transforming utility operations by enabling real-time decision-making, automating high-risk inspections, and streamlining reporting and communications. All while remaining increasingly accessible, scalable, and cost-effective.

Labour and safety: Addressing workforce challenges

Utilities face workforce shortages and safety risks, and AI-driven automation helps by handling inspections, monitoring equipment, and training staff, reducing hazards while maintaining reliability.

Economic efficiency: Doing more with less

Amid rising costs, AI boosts utility efficiency through predictive maintenance, automated service, and intelligent forecasting, driving long-term value and sustainability. In an era of rising operational costs and constrained capital budgets, utilities are under pressure to maximize efficiency. AI is a strategic lever for achieving this. Predictive maintenance reduces costly downtime, automated customer service improves satisfaction while lowering overhead, and intelligent forecasting enhances financial planning. These efficiencies compound over time, turning AI from a cost centre into a value generator. For utilities looking to balance innovation with fiscal responsibility, AI offers a pathway to long-term sustainability.

Current landscape and future outlook

Currently, AI is used for grid analytics, predictive maintenance, and customer service automation. Drones are deployed for line inspections, vegetation management, and storm assessments. Robotics are emerging in substation automation and hazardous environment operations. Looking ahead, AI investment is expected to double globally by 2026, with Canadian utilities aligning their strategies accordingly. Integration with augmented reality/virtual reality and smart grid systems is anticipated. However, rising costs driven by inflation, labour shortages, and supply chain issues pose a significant challenge to widespread adoption.

Opportunities

AI is rapidly emerging as a strategic enabler for Canadian electric utilities, driving transformation across grid modernization, customer experience, productivity, and safety. In grid modernization, AI is being used to analyze outage patterns, optimize power flow models and generate grid insight by integrating data from systems like Advanced Distribution Management Systems (ADMS) and Geographic Information System (GIS). Drones equipped with vision AI can be used to inspect remote assets and identify vegetation risks, improving asset condition monitoring and informing proactive maintenance strategies.

Customer experience and operational productivity can be elevated through intelligent agents that automate call summarization, classify service requests, and support compliance monitoring. Agentic AI—an advanced combination of robotics and generative AI, can autonomously plan, make decisions, and act with minimal human input. These agents enhance call centre efficiency by reducing manual review time and improving service quality.

Safety and compliance can be further strengthened through AI-driven quality checks and contextual safety guidance for field crews. Robotic systems with virtual reality AI capabilities are also being deployed in substations and hazardous environments to perform inspections and maintenance, minimizing human exposure and improving safety outcomes. Regulatory intelligence agents assist with rate filings and incident investigations, while generative AI supports schematic validation and asset record verification. Together, these innovations in AI, robotics, and drones can modernize utility operations and safety and meet evolving regulatory and customer expectations.

Challenges and risks

The adoption of AI, robotics, and drone technologies in the utility sector presents several interconnected challenges. Rising costs are a key concern, especially as many AI solutions rely on cloud infrastructure, which is treated as operational expenditure (OPEX). Managing cloud expenses effectively is critical, and regulatory changes around the financial treatment of cloud investments will play a significant role in enabling broader adoption.

Cybersecurity risks are heightened with the integration of AI, robotic systems, and drones, increasing exposure to threats across both IT and OT environments. These technologies introduce new vulnerabilities related to data security and OT asset protection. An assessment of each technology's cybersecurity impact must be conducted prior to deployment, and appropriate controls and safeguards must be built into the implementation process. Establishing a robust AI governance framework is essential to ensure secure, responsible, and compliant use of intelligent systems.

Trust and interoperability also pose significant barriers. Poor data quality and fragmented data ownership hinder AI effectiveness. A comprehensive data strategy is essential—one that includes strong data governance to define ownership, enforce quality standards, and break down silos. Investing in data foundation technologies will improve accessibility. Additionally, promoting a data-driven culture across the organization is important to drive adoption of these technologies. Increasing AI literacy through targeted AI education will empower staff to engage with AI tools confidently and responsibly. Establishing an innovation lab can provide a safe environment to experiment with advanced technologies and foster cross-functional collaboration.

Strategic recommendations

Invest in governance: Establish clear AI and robotics governance frameworks to manage risk and ensure ethical use

Collaborate across utilities: Share best practices and co-develop standards through industry bodies like Electricity Canada

Prioritize cybersecurity: Integrate AI-ready security protocols from the outset

Upskill the workforce: Invest in training programs to build internal AI and robotics expertise

Pilot and scale: Start with small-scale pilots to validate ROI before full deployment.

Embed AI in strategy: Align AI initiatives with business outcomes and regulatory goals

Conclusion

In conclusion, the convergence of AI, robotics, and drone technologies marks a thrilling chapter in the evolution of Canada's electric utility sector. These innovations are not only reshaping how utilities operate but are also unlocking new possibilities for resilience, efficiency, and customer engagement. As these technologies continue to mature and integrate, they promise to deliver transformative value—empowering utilities to meet the challenges of tomorrow with agility and vision. The future is bright, and the journey ahead is filled with opportunity and innovation.

Major systems migrations

Major systems migrations

Contributing authors:

- **Ana Lalic**, Senior Program Manager, BC Hydro
- **Loan Kenny**, Acting Chief Enterprise Architect, BC Hydro
- **Nada Kovacevic**, Director, Enterprise Solutions and Analytics, BC Hydro
- **Davor Razlog**, Director, Technology Delivery, BC Hydro

Overview

As companies modernize their digital platforms and broader technology environments, they are undertaking greater technology system upgrades and migrations. The magnitude and complexity of these initiatives differ from routine upgrades to major resource-intensive overhauls.

The current wave of upgrades and migrations typically involves platform and product changes, adopting a new generation of products, transforming business processes, and unlocking new capabilities made possible by technological advancements such as generative AI, cloud computing, built-in best practices, and the evolving collaborative nature of work.

Impacted Systems

Enterprise resource planning (ERP), enterprise asset management, extended Relationship Management, telephony, and extend to operating technologies such as Energy Management Systems, Automated Metering Infrastructure, Advanced Distribution Management Systems, and Geographic Information Systems and more.

Key drivers

Changing business models and platforms

Vendor-imposed upgrades leave organizations with few options other than to upgrade and migrate. With the next generation of products already available, vendors are actively pushing customers towards their new solutions. They are taking a firm position on sunsetting support for systems used in critical business processes.

On the other hand, some vendors are struggling to present compelling visions and roadmaps for their products, prompting organizations to consider replacement. Migrations may also be triggered by changes in licensing models and pricing strategies aimed at increasing vendor revenue without providing additional value to customers.

Cloud adoption

The adoption of cloud technologies and the desire to reduce the internal data centre footprint drives some migrations. These initiatives are typically part of a broader cloud strategy and internally initiated. Many vendors are increasingly innovating and providing new features

exclusively in the cloud, making cloud implementations more appealing than traditional on-premise solutions.

Obsolescence

Work and the expectations of the modern workforce are evolving, and analog and/or digital tools are no longer keeping pace with changing business processes. While incremental improvements have sustained operational solutions for years, some legacy tools are no longer fit for purpose and must be updated to function in a more modern system-integrated environment.

Merger and acquisition consolidation

Organizations with many subsidiaries or recent acquisitions may consider driving harmonization and alignment of business processes and tools through major system implementations across their entities.

Challenges and risks

Utilities undertaking major system migrations should plan holistically, aligning with their target architecture and sequencing projects to reduce complexity and risk. Phased approaches can reduce risk for large initiatives, while early migration is often preferable to meet end-of-life deadlines and realize benefits sooner. Organizations must reassess legacy customizations, ensure strong data quality and governance, and carefully evaluate cloud adoption trade-offs. Workforce impacts should be anticipated with training and temporary support, and robust project delivery practices including independent oversight are critical to success. Early user engagement, iterative development, and multiple rehearsals can improve adoption and cutover outcomes. Finally, utilities must manage rising implementation and operating costs, particularly subscription-based licensing, through careful contract oversight and, where appropriate, regulatory engagement.

Planning and architecture: Inadequate alignment with the organization's future technology environment, poorly sequenced migration steps, or lack of comprehensive roadmaps can lead to inefficient migrations, missed opportunities for integration, and potential system incompatibilities across IT, OT, and business units.

Complexity and customization: Extensive legacy system customizations, the need to adjust business processes for off-the-shelf solutions, and cloud platform limitations can increase migration difficulty, delivery risks, user resistance, and the likelihood of project rework or reimplementation.

Data and cloud: Poor data quality, lack of governance, or delayed cleansing efforts can propagate errors into new systems, while cloud migrations may require trade-offs in features, create new OPEX costs, or introduce dependencies on vendor platforms that could affect long-term flexibility and scalability.

Operational and workforce: Migration impacts can temporarily reduce productivity, strain staff capacity, require extensive training, and face retention challenges as employees gain new, highly marketable skills; these factors can affect service delivery and adoption of new systems.

Delivery and oversight: Insufficient project management practices, weak oversight, or underprepared delivery partners and system integrators increase the likelihood of missed deadlines, implementation errors, ineffective change management, and compromised quality during deployment and cutover activities.

Financial and licensing: Rising implementation costs, complex subscription and licensing models, market-driven vendor pricing, and higher operating costs for new systems can strain budgets, reduce ROI, and require careful contract management or regulatory negotiation to control expenses.

Strategic recommendations

Proactively develop strategies and plans: With a growing volume of migrations and upgrades becoming inevitable, utilities need to address both market-driven and internally initiated migrations and upgrades. Since the impacts extend beyond just technology teams, all parts of the business need to be actively involved in shaping the strategy development and governance framework.

Focus resources on key business process changes: Strategies will include business process changes, as well as address any gaps in resourcing capacity and capability across both business and technology teams. Dedicating a smaller number of full-time resources from each area to these initiatives is often more effective than spreading resources across multiple priorities.

Engage multiple partners for large-scale migrations: Internal teams may need to be complemented with reputable and experienced implementation partners, so procurement approaches and strategies will be needed as well. It is unlikely that a single implementation partner will be able to support all migration needs due to the volume and broad areas involved.

Learn from peers to improve migration planning: Utilities could connect with the network of similar organizations to understand the lessons learned and lean on during challenges through planning and implementation.

Executives must guide strategy and migration decisions: Strong executive-level governance and oversight should be established to guide both strategy development and migration implementation. Involving key executives in critical decision-making, escalation handling and strategic direction, helps minimize churn that often happens during such large initiatives.

Conclusion

Organizations must undertake major system migrations to modernize environments, support critical processes, and unlock new capabilities. Well-defined plans, governance, and enterprise architecture roadmaps help manage risks, guide timing and scope, and ensure successful delivery, while robust project practices and cross-organizational engagement address productivity impacts and system stabilization.

Trends in cybersecurity

Trends in cybersecurity

Authors:

- **Alex Foord**, CIO, Independent Electricity System Operator
- **Norm Van Bergen**, Senior Specialist, Information Security

Overview

Cyberthreats to Canada's electricity sector are escalating in complexity, while regulatory mandates are reflecting increased scrutiny of the sector's cybersecurity posture. With ransomware and vulnerability exploitation increasing, AI offers both risk at the hands of threat actors and opportunities at the hands of defenders. Rising breach costs are influencing strategic investments. Organizations are now working to balance operational resilience with financial constraints, leverage innovation to mitigate risk, and enhance cyber incident prevention, detection and incident response.

Key drivers

Regulatory: Sector regulators are taking a more active role in understanding, analyzing, and considering the impacts of cybersecurity. For example, the Ontario Energy Board (OEB) has directed that periodic third-party cybersecurity assessments will be undertaken and funded by licenced transmitters and distributors within the province and submitted to the OEB. Additionally, the OEB is mandating cybersecurity incident reporting for these organizations, highlighting how one regulator is signifying an elevated and persistent focus on the importance of cyber risk management activities. Doing so seeks to increase sector-wide information exchange, improve threat detection and response, and support continuous improvement within sector's cyber strategies and practices.

Cybercrime: Cyber gangs are leveraging cybercrime to seek financial gains for personal profit, while some nation-state actors are utilizing stolen/extorted funds to support their strategic objectives. This can include compensating for the impacts of economic sanctions, supporting military and political ambitions, and providing capital to further perform their cyber operations.

Artificial intelligence: The rapid evolution of AI is serving to amplify the threats in cyberspace through more effective tools and improving criminals' techniques to exploit their victims, while making detection of their activities more difficult (IBM, 2024).

Conversely, AI can enable and support more effective threat detection and incident response within organizations that have the tooling and skills to leverage it. By augmenting human expertise, analysis, and decision-making, AI can increase bandwidth in security operations teams, helping elevate accuracy and reduce cycle times to detect potential incidents sooner and respond to them in less time (McKinsey & Company, 2025). IBM identified that AI could help lower breach costs in some instances by an average of US$2.2 million (IBM, 2024).

Quantum computing: The evolution of quantum computing technologies has resulted in the Canadian Centre for Cyber Security (CCCS) predicting that sufficiently powerful quantum-based systems to break today's cryptography will exist by the 2030s[i]. Some advanced threat actors are

assumed to be taking the approach of "steal now, decrypt later," leveraging forthcoming quantum computing capabilities to break the encryption currently protecting stolen data.

Insider risk: Threat actors are directing more resources to influence the human element of the technology chain. Acting alone or under direction, compromised employees and contractors may intentionally misuse their access for financial gain, revenge, espionage, or sabotage. Malicious insider attacks resulted in cyber incident costs averaging US$4.99 million per incident (IBM, 2024).

Geopolitics: Geopolitics has a growing role in influencing the cybersecurity posture of organizations due to changes in the threat landscape affected by nation-state conflicts, sanctions, trade wars, and evolving international partnerships. When frictions arise due to these factors, there may be targeted cyberattacks, increased supply chain vulnerabilities, and other impacts. China's expansive and aggressive cyber program is the most comprehensive cybersecurity threat facing Canada today (CCCS, 2024).

Current landscape and future outlook

Increasing cyber risks: The latest CCCS National Threat Assessment (CCCS, 2024) states the number, severity, complexity, and sophistication of cyber incidents has increased sharply over the past two years. These are considered to now extend beyond espionage to include capabilities to disrupt environments through manipulation of systems, data destruction/exfiltration, and more. Should a military conflict occur, civilian infrastructure is now considered a legitimate target.

Ransomware: Ransomware is the single largest cybercrime threat to critical infrastructure in Canada today. The CCCS reports an average annual increase of 26 per cent in ransomware incidents across all Canadian sectors from 2021 through the projected end of 2024 (CCCS, 2024).

Exploitation of vulnerabilities: The number of system vulnerabilities disclosed in 2024 was over 30,000 – an increase of 17 per cent over the previous year[ii]. Threat actors are leveraging these vulnerabilities, sometimes leveraging AI to magnify their efforts.

Artificial intelligence: In 2024, the number of organizations using AI grew by slightly more than 10 per cent year-over-year. Organizations extensively leveraging AI for cyber defense reported that they identified and contained data breaches nearly 100 days faster on average than organizations that didn't (IBM, 2024), thereby shortening detection and containment times while also lowering breach costs.

Cybersecurity investments are rising: Global cybersecurity spending is predicted to increase by slightly over 12 per cent in 2025. Increases are being driven largely by additional investments in cloud application protections, Identity and Access Management (IAM), security analytics, and incident response planning/testing (IDC, 2025) (IBM, 2024). As a percentage of overall IT spending, cybersecurity typically accounts for approximately 13 per cent of overall IT budgets, up from 8.6 per cent in 2020 (The National CIO Review, 2024).

Inflection point:

Adoption of artificial intelligence: The emergence of AI, combined with its rapid development and the associated hype cycle, has many companies finding themselves at a crossroads. They can either embrace AI wholesale, adopt it gradually, or take a 'wait and see' approach based on evolving guidance and what other sector leaders are doing.

Opportunities

Despite the financial challenges and increasing cyber hazards facing organizations today, opportunities exist to increase efficiency and to lower some risks through strategic focus on key cyber resource allocations. Doing so not only strengthens grid security and resilience but also reinforces the energy foundations that support Canadian growth through trade diversification and decarbonization, while showcasing thought leadership and technological innovation within the sector.

Leveraging AI should also be considered as a force-multiplier as part of an organization's security processes and tooling. For example, AI-enhanced penetration testing can increase the effectiveness of identifying potential security gaps and vulnerabilities.

Challenges and risks

Increasing and hidden data reach costs: According to IBM's "Cost of a Data Breach Report," the global average cost of a data breach *increased* 10 per cent over the previous year, reaching US$4.88 million (IBM, 2024). Business disruption impacts and post-incident response activities comprised most of these annual cost increases**.** The obscured costs of a data breach are often underestimated and can include response/recovery time, impact to customers, legal/regulatory impacts, and reputational damage to name a few. These hidden financial impacts were a material contributor to the financial burden of a breach borne by a recently impacted Canadian integrated utility that was the target of ransomware.

Risks of under-funding cybersecurity programs: Organizations should consider the potential negative impacts on enterprise risk if security funding does not provide the support required to meet evolving and rising challenges.

Strategic recommendations

Implement artificial intelligence: Leaders should consider the strategic integration of AI capabilities into their business processes and their cybersecurity program. They should focus on approved use cases, effective governance, and the establishment of meaningful KPIs to generate measurable ROI. To help mitigate risk, AI systems (notably their prompt interfaces) should be included as penetration testing targets to help identify vulnerabilities, configuration errors, confirm model integrity, and ensure alignment with security policies and standards.

Threat intelligence for vulnerability management: This supports more effective prioritization of patching/upgrade activities, helping to lower the risk of a breach based on the knowledge of threat actors' exploitations of known vulnerabilities.

Quantum computing considerations: Organizations should consider investing now to review and assess their current data assets and protections, with the intention to upgrade appropriate elements of their encryption standards to certified “quantum-safe” algorithms (generally referred to as “Post Quantum Cryptography”).

Geopolitical risk intelligence: With the growing intersection of geopolitics and cybersecurity, organizations should consider incorporating geopolitical risk intelligence into their cybersecurity strategies and processes to provide an additional line-of-sight.

Review and update insider risk management strategies: Consider additional processes and controls across the entire resource lifecycle for key employees that have access to sensitive systems and data. To better support detection and response to both accidental and intentional data exfiltration, explore the implementation of a data loss protection (DLP) program to help identify, manage, and mitigate these types of incidents. Consideration should be given to the use of AI-enhanced systems, such as behavioral analytics, to further help in detecting potential malicious insider-threat activities.

Conclusion

The Canadian electricity sector faces a rapidly evolving cyberthreat landscape, with increasing ransomware, vulnerabilities, and sophisticated nation-state activity driving the need for stronger defenses. By strategically leveraging AI, threat intelligence, quantum-safe encryption, geopolitical risk insights, and enhanced insider risk management, utilities can strengthen resilience, reduce breach costs, and protect critical infrastructure while maintaining operational and regulatory compliance.

Summary

The convergence of technological innovation, digital transformation, and operational modernization presents Canadian electricity providers with major opportunities. Across citizen development, AI and robotics, major systems migrations, and cybersecurity, a clear pattern emerges: companies must balance innovation, resilience, and security while leveraging data-driven insights, workforce enablement, and enterprise-wide collaboration and remain cost effective with increasing costs and other financial risks.

To succeed in this evolving landscape, utilities should act decisively through:

- **Investing in people and skills:** Build internal capability through continuous training, AI literacy, and cross-functional engagement to empower employees and citizen developers.
- **Strengthening governance and security:** Implement robust cybersecurity frameworks, risk management, and AI governance to protect critical infrastructure and data.
- **Modernizing systems strategically:** Plan and execute system migrations and digital transformations in alignment with enterprise architecture, cloud strategies, and operational priorities.
- **Fostering innovation and collaboration:** Encourage collaboration across IT, OT, and business units to unlock operational efficiencies, improve customer experience, and accelerate climate-resilient solutions.
- **Leveraging data and technology:** Adopt AI, robotics, drones, and low-code/no-code platforms to improve decision-making, optimize operations, and drive sustainable growth.

By taking these actions, utilities can transform challenges into opportunities, creating a more agile, secure, and innovative electricity sector that meets regulatory expectations, enhances resilience, and positions Canada’s energy system for a sustainable, technology-enabled future.

Bibliography

Canadian Centre for Cyber Security (CCCS). (2024). *National Cyber Threat Assessment 2025-2026.* Communications Security Establishment Canada.

IBM. (2024). *Cost of a Data Breach Report.*

IDC. (2025, March 21). *Worldwide Security Spending to Increase by 12.2% in 2025*. Retrieved from https://my.idc.com/getdoc.jsp?containerId=prEUR253264525

McKinsey & Company. (2025). *Technology Trends Outlook 2025.*

The National CIO Review. (2024, September 26). *The Cost of Good Security: Analyzing 2024's Cyber Budget Trends*. Retrieved from https://nationalcioreview.com/articles-insights/information-security/the-cost-of-good-security-analyzing-2024s-cyber-budget-trends/

[i] https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017
[ii] https://cybersecuritynews.com/2025-cybersecurity-trends/


Electricity Canada
Électricité Canada
electricity.ca